FIG. 1

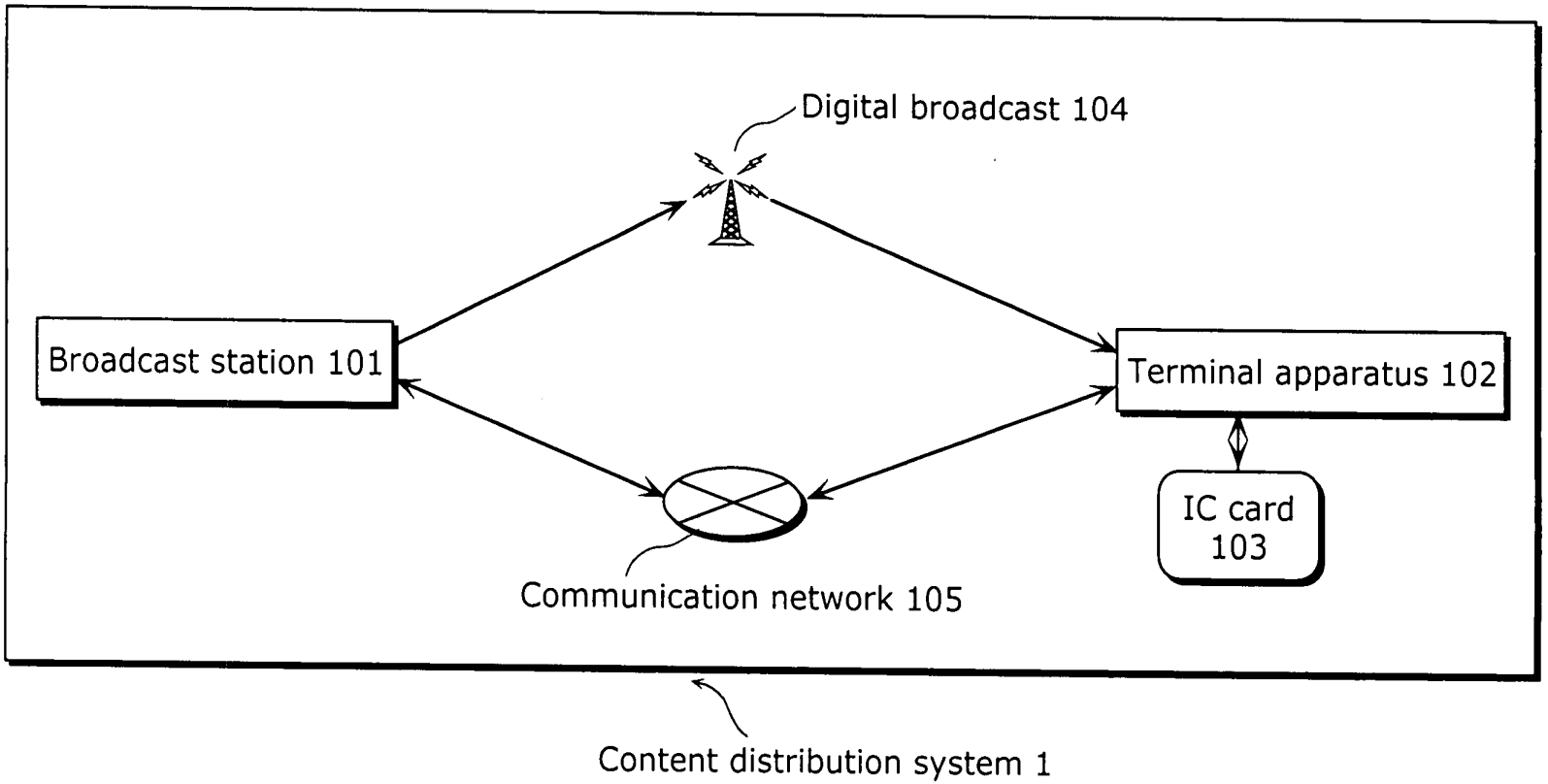

Digital broadcast 104
Broadcast station 101
Terminal apparatus 102
IC card
103
Communication network 105
Content distribution system 1

FIG. 2

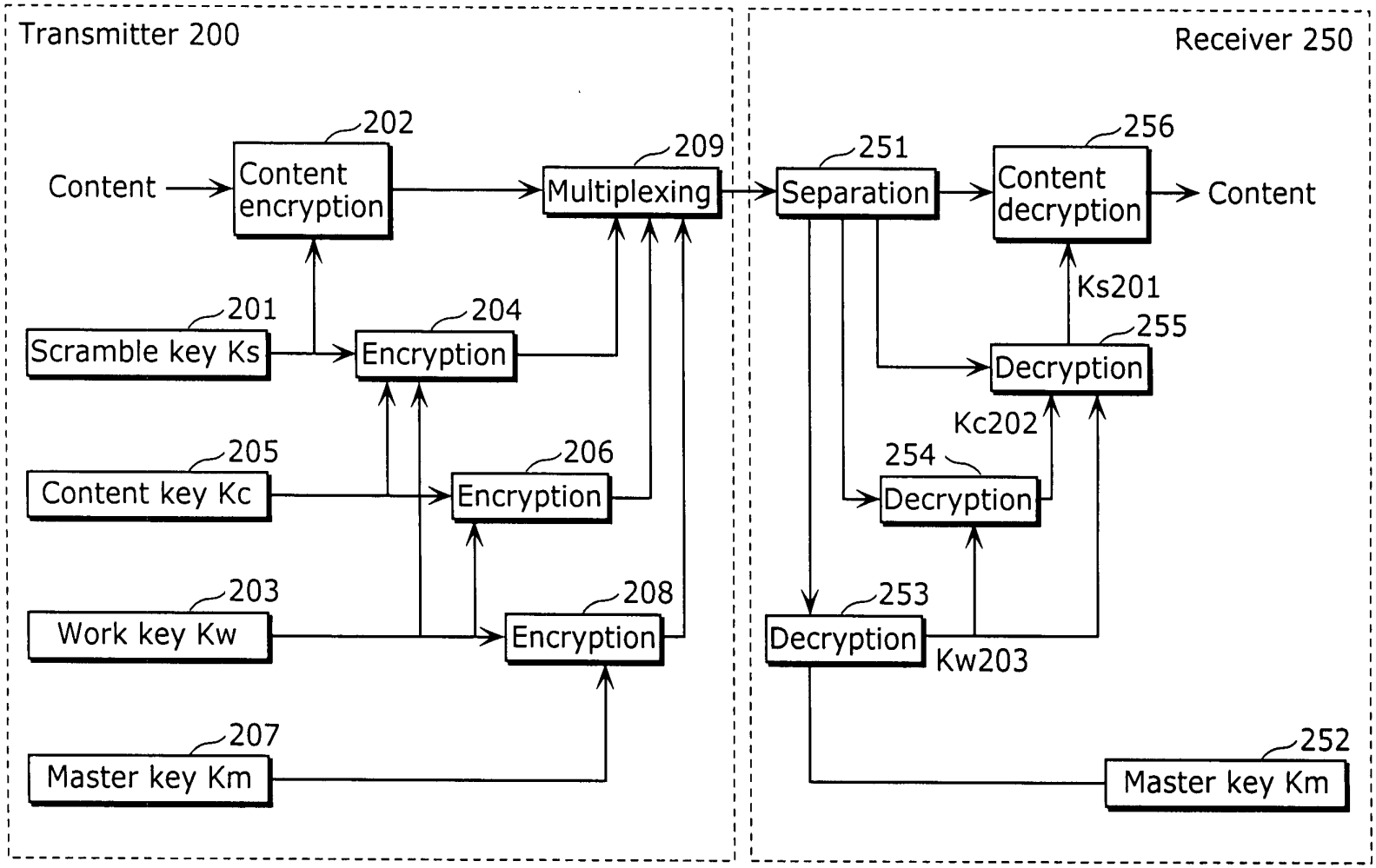

Transmitter 200
Receiver 250
Content
202
Content encryption
209
Multiplexing
251
Separation
256
Content decryption
Content
201
Scramble key Ks
204
Encryption
Ks201
255
Decryption
Kc202
205
Content key Kc
206
Encryption
254
Decryption
203
Work key Kw
208
Encryption
253
Decryption
Kw203
207
Master key Km
252
Master key Km

FIG. 3

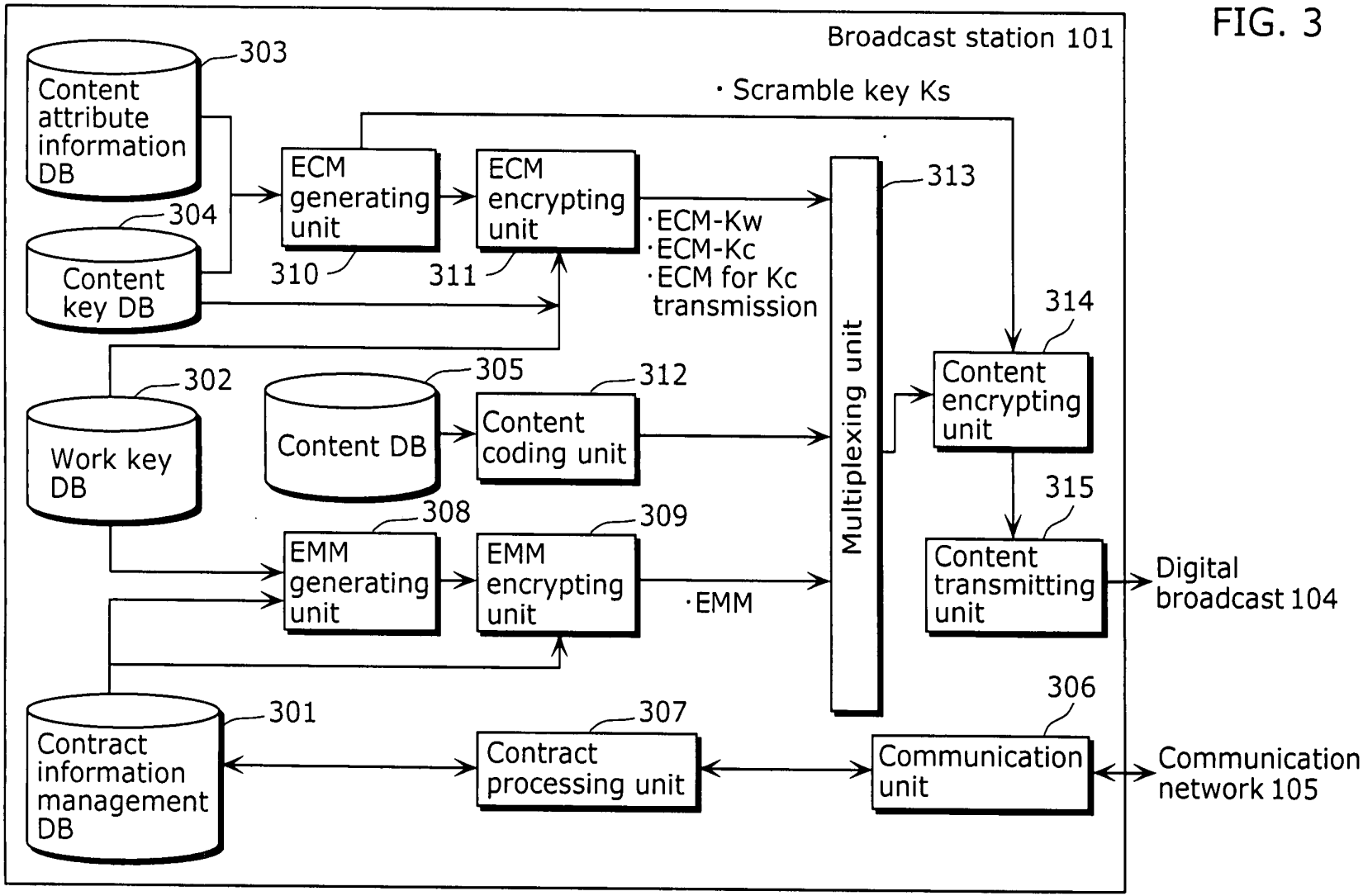

Broadcast station 101
303
Content attribute information DB
304
Content key DB
302
Work key DB
305
Content DB
308
EMM generating unit
309
EMM encrypting unit
301
Contract information management DB
ECM generating unit
310
ECM encrypting unit
311
· Scramble key Ks
· ECM-Kw
· ECM-Kc
· ECM for Kc transmission
· EMM
312
Content coding unit
313
Multiplexing unit
314
Content encrypting unit
315
Content transmitting unit
Digital broadcast 104
307
Contract processing unit
306
Communication unit
Communication network 105

FIG. 4

401 Card ID	402 Tier contract ID	403 PPV contract ID	404 Validity period	405 Stored encryption key Km'	406 Master key Km
CARD-ID-1	TIERCONT-ID-1	PPVCONT-ID-1	2004/4/1～ 2005/3/31	0x111・・・111	0x111・・・111
CARD-ID-2	TIERCONT-ID-1	PPVCONT-ID-2	2003/12/1～ 2004/11/30	0x222・・・222	0x222・・・222
CARD-ID-3	TIERCONT-ID-2	PPVCONT-ID-1	2004/1/1～ 2004/4/30	0x333・・・333	0x333・・・333
CARD-ID-4	TIERCONT-ID-3	PPVCONT-ID-1	2004/1/1～ 2005/3/31	0x444・・・444	0x444・・・444
・・・	・・・	・・・	・・・	・・・	・・・

Contract information management table 400

FIG. 5

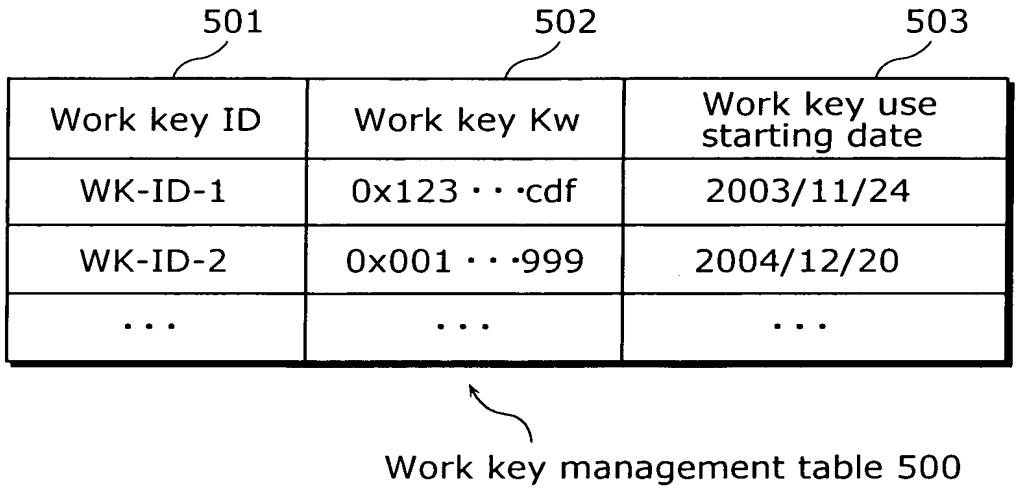

501
502
503
Work key ID
Work key Kw
Work key use starting date
WK-ID-1
0x123 · · ·cdf
2003/11/24
WK-ID-2
0x001 · · ·999
2004/12/20
· · ·
· · ·
· · ·
Work key management table 500

FIG. 6

601 Content ID	602 License ID	603 Use condition	604 Contract information	605 License transformation period
CONTENT-ID-1	LICENSE-ID-1	Validity period: 1 month	TIERCONT-ID-1	2004/4/30
CONTENT-ID-2	LICENSE-ID-2	Validity period: 1 month. Reproduction frequency: 10 times	TIERCONT-ID-1 TIERCONT-ID-2	2004/4/15
CONTENT-ID-3	LICENSE-ID-3	Validity period: 3 months	TIERCONT-ID-1	2004/4/25
CONTENT-ID-4	LICENSE-ID-4	Validity period: 3 days. Writing frequency: once	PPVCONT-ID-1	2004/5/1
...	...	...		...

Content attribute information management table 600

FIG. 7

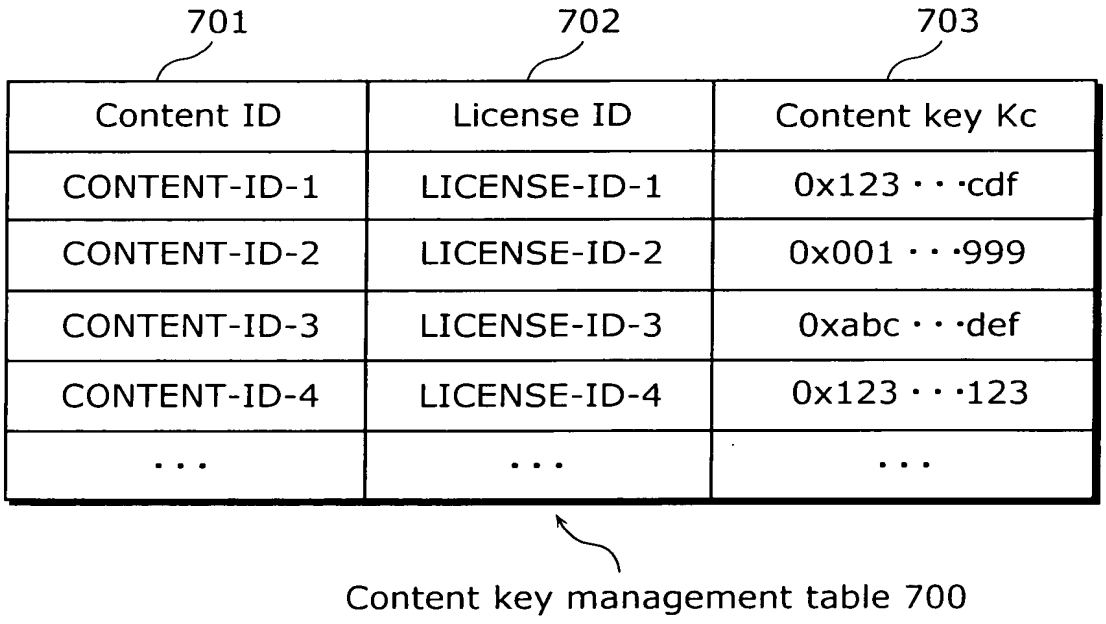
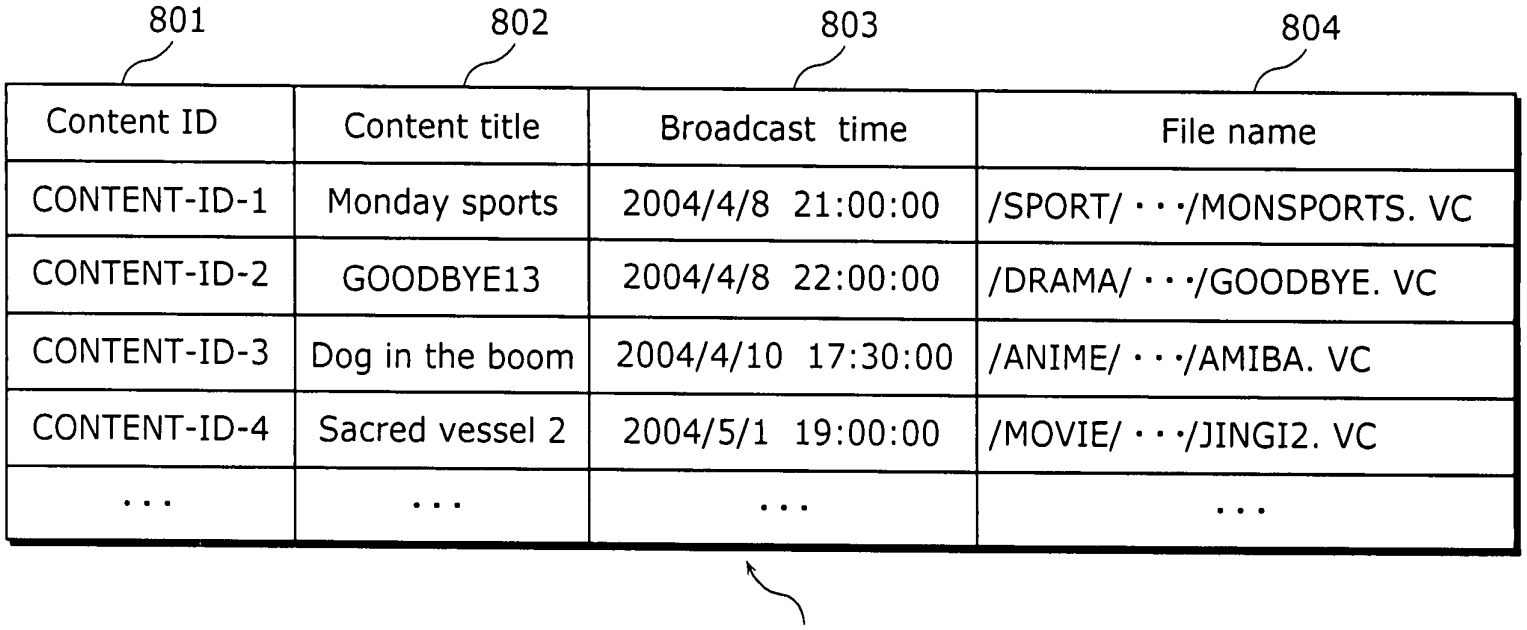

701
702
703
Content ID
License ID
Content key Kc
CONTENT-ID-1
LICENSE-ID-1
0x123 · · ·cdf
CONTENT-ID-2
LICENSE-ID-2
0x001 · · ·999
CONTENT-ID-3
LICENSE-ID-3
0xabc · · ·def
CONTENT-ID-4
LICENSE-ID-4
0x123 · · ·123
· · ·
· · ·
· · ·
Content key management table 700

FIG. 8



Content management table 800

FIG. 9

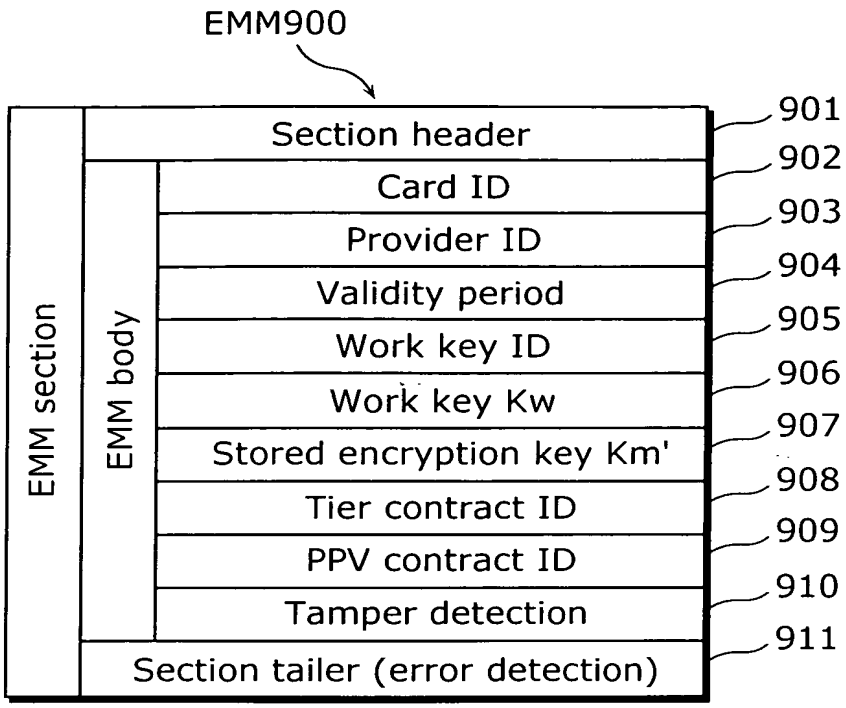

EMM900
EMM section
EMM body
Section header
Card ID
Provider ID
Validity period
Work key ID
Work key Kw
Stored encryption key Km'
Tier contract ID
PPV contract ID
Tamper detection
Section tailer (error detection)
901
902
903
904
905
906
907
908
909
910
911

FIG. 10

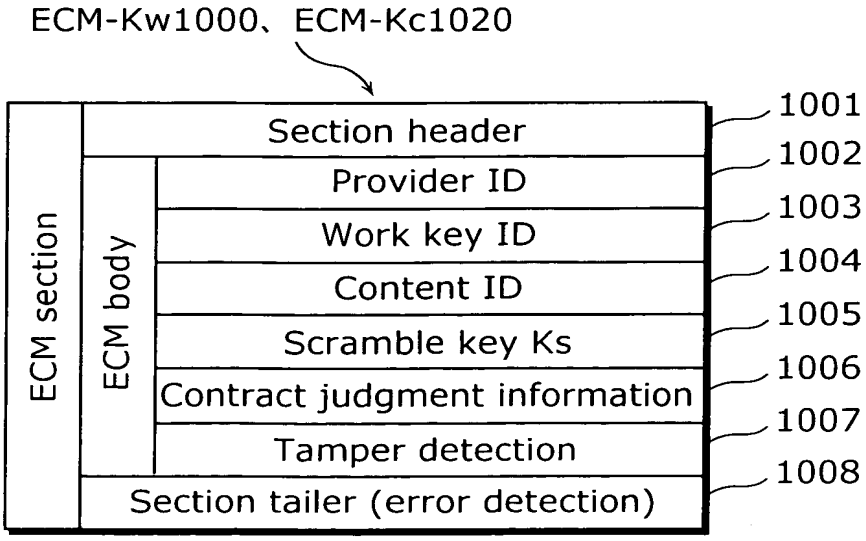

ECM-Kw1000、ECM-Kc1020
ECM section
ECM body
Section header
Provider ID
Work key ID
Content ID
Scramble key Ks
Contract judgment information
Tamper detection
Section tailer (error detection)
1001
1002
1003
1004
1005
1006
1007
1008

FIG. 11

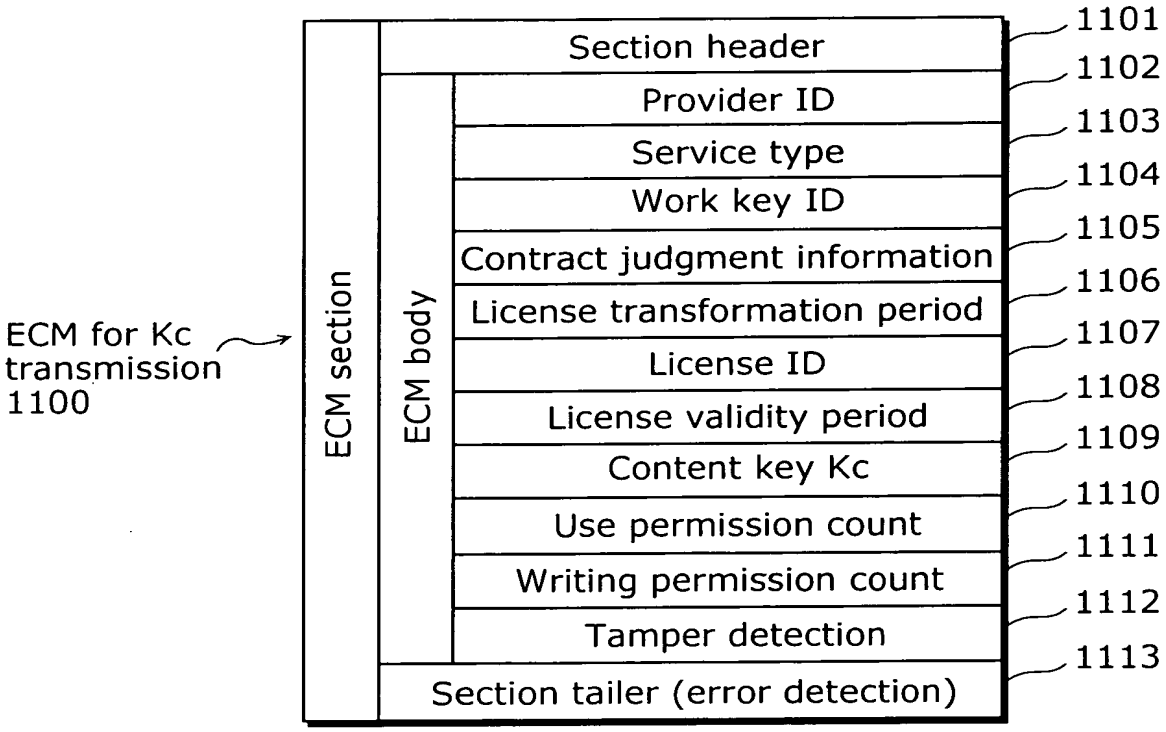

ECM for Kc transmission 1100
ECM section
ECM body
Section header
Provider ID
Service type
Work key ID
Contract judgment information
License transformation period
License ID
License validity period
Content key Kc
Use permission count
Writing permission count
Tamper detection
Section tailer (error detection)
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113

FIG. 12

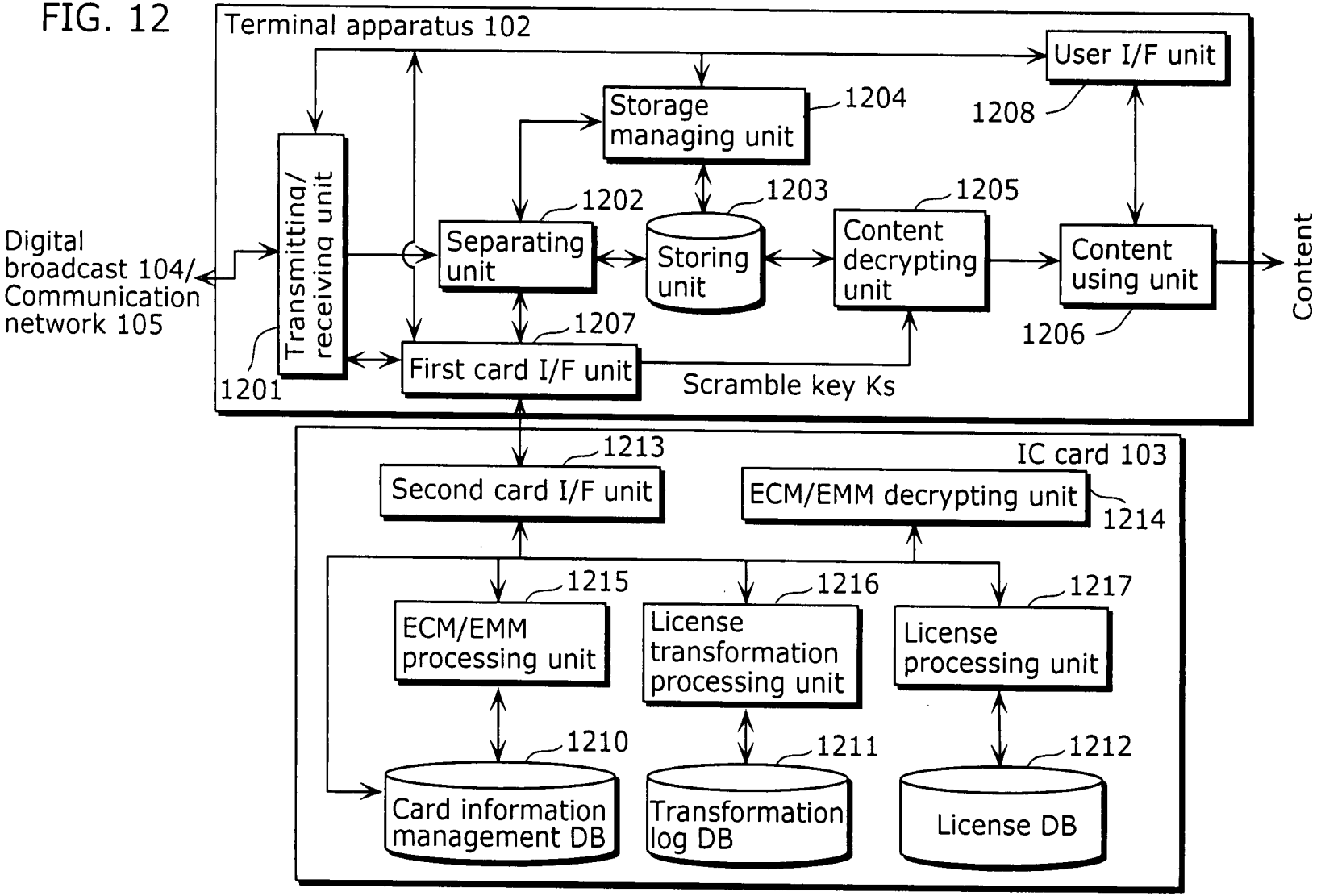

Terminal apparatus 102
User I/F unit
1208
Storage managing unit
1204
Transmitting/ receiving unit
1202
1203
1205
Digital broadcast 104/ Communication network 105
Separating unit
Storing unit
Content decrypting unit
Content using unit
Content
1207
1206
1201
First card I/F unit
Scramble key Ks
IC card 103
1213
Second card I/F unit
ECM/EMM decrypting unit
1214
1215
1216
1217
ECM/EMM processing unit
License transformation processing unit
License processing unit
1210
1211
1212
Card information management DB
Transformation log DB
License DB

FIG. 13

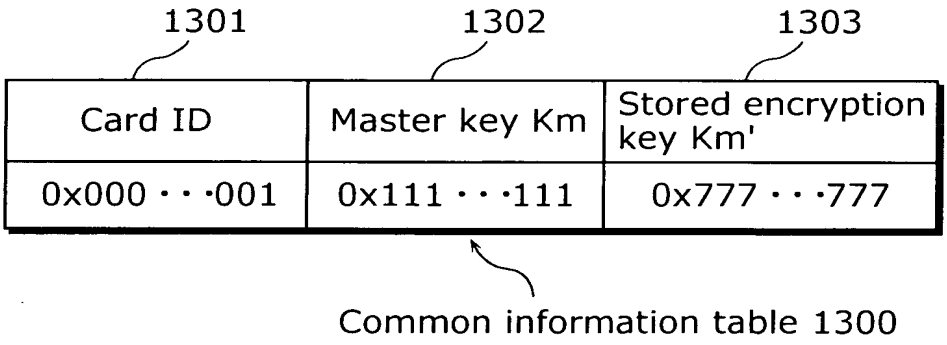

1301
1302
1303
Card ID
Master key Km
Stored encryption key Km'
0x000 · · ·001
0x111 · · ·111
0x777 · · ·777
Common information table 1300

FIG. 14

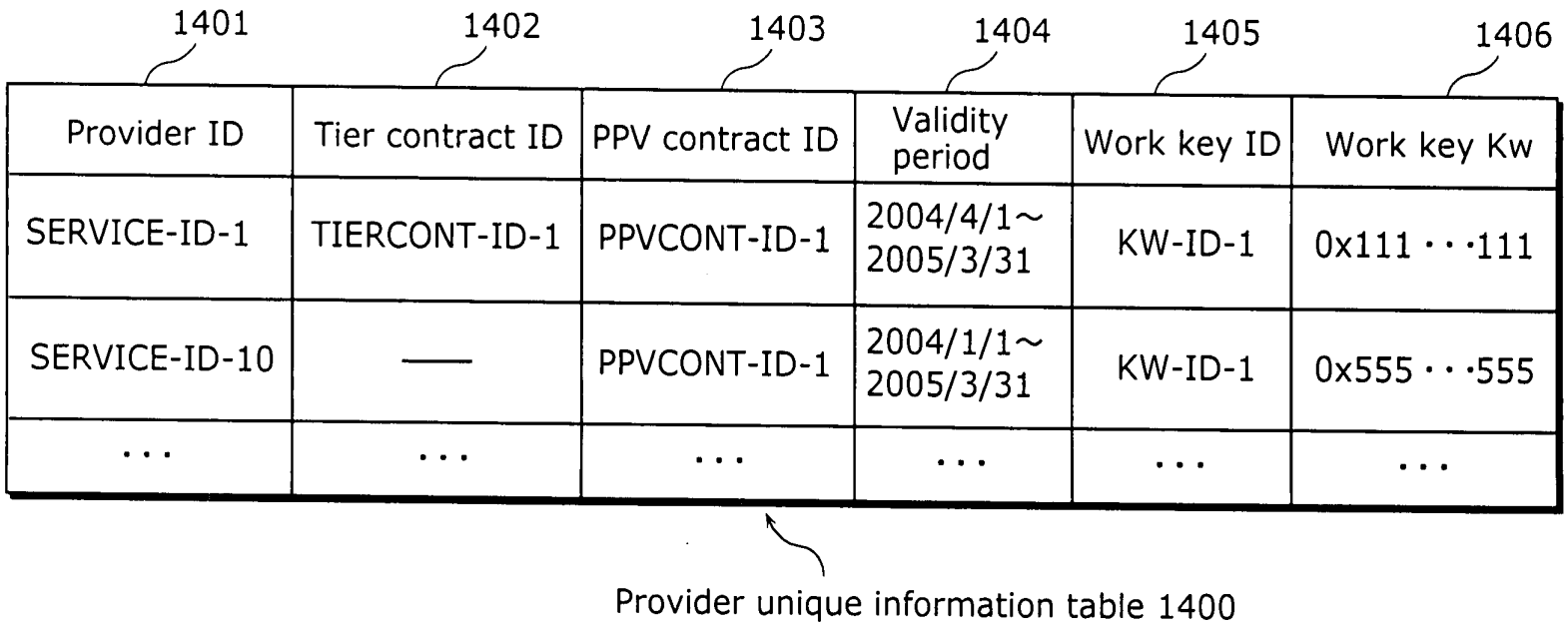

1401
1402
1403
1404
1405
1406
Provider ID
Tier contract ID
PPV contract ID
Validity period
Work key ID
Work key Kw
SERVICE-ID-1
TIERCONT-ID-1
PPVCONT-ID-1
2004/4/1~ 2005/3/31
KW-ID-1
0x111・・・111
SERVICE-ID-10
——
PPVCONT-ID-1
2004/1/1~ 2005/3/31
KW-ID-1
0x555・・・555
・・・
・・・
・・・
・・・
・・・
・・・
Provider unique information table 1400

FIG. 15

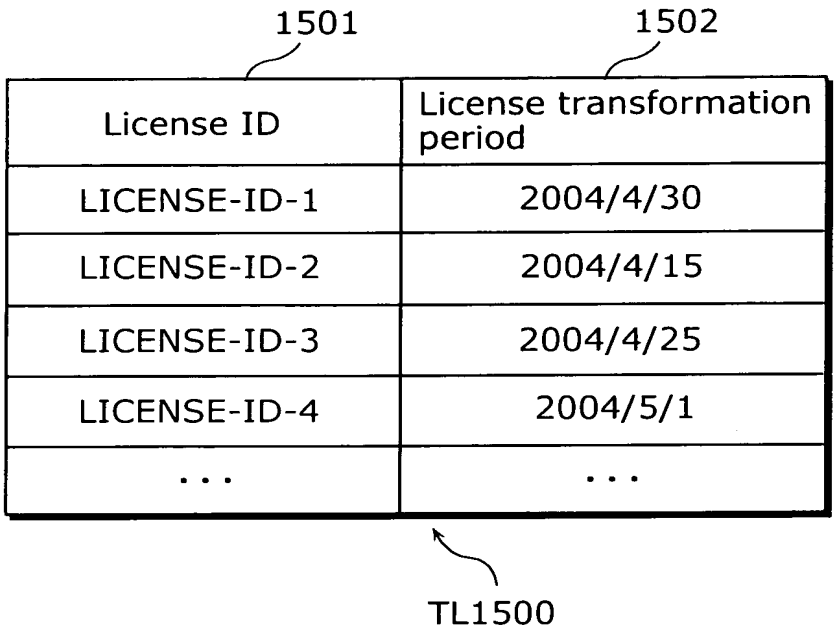

1501
1502
License ID
License transformation period
LICENSE-ID-1
2004/4/30
LICENSE-ID-2
2004/4/15
LICENSE-ID-3
2004/4/25
LICENSE-ID-4
2004/5/1
TL1500

FIG. 16

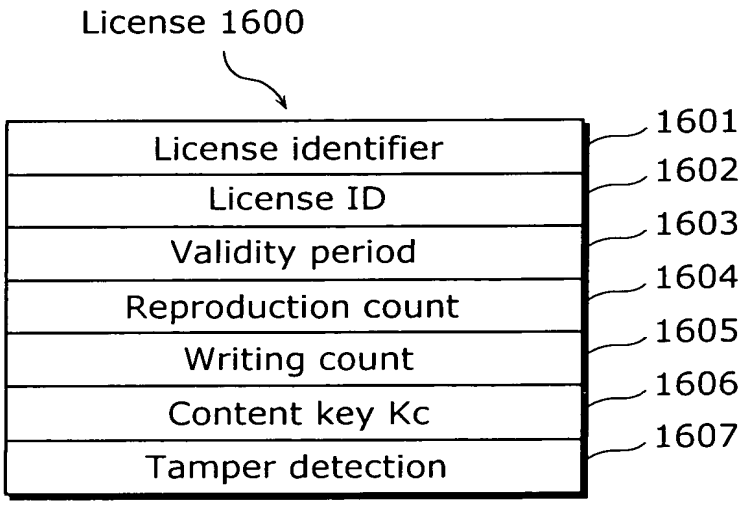

License 1600
License identifier
License ID
Validity period
Reproduction count
Writing count
Content key Kc
Tamper detection
1601
1602
1603
1604
1605
1606
1607

FIG. 17

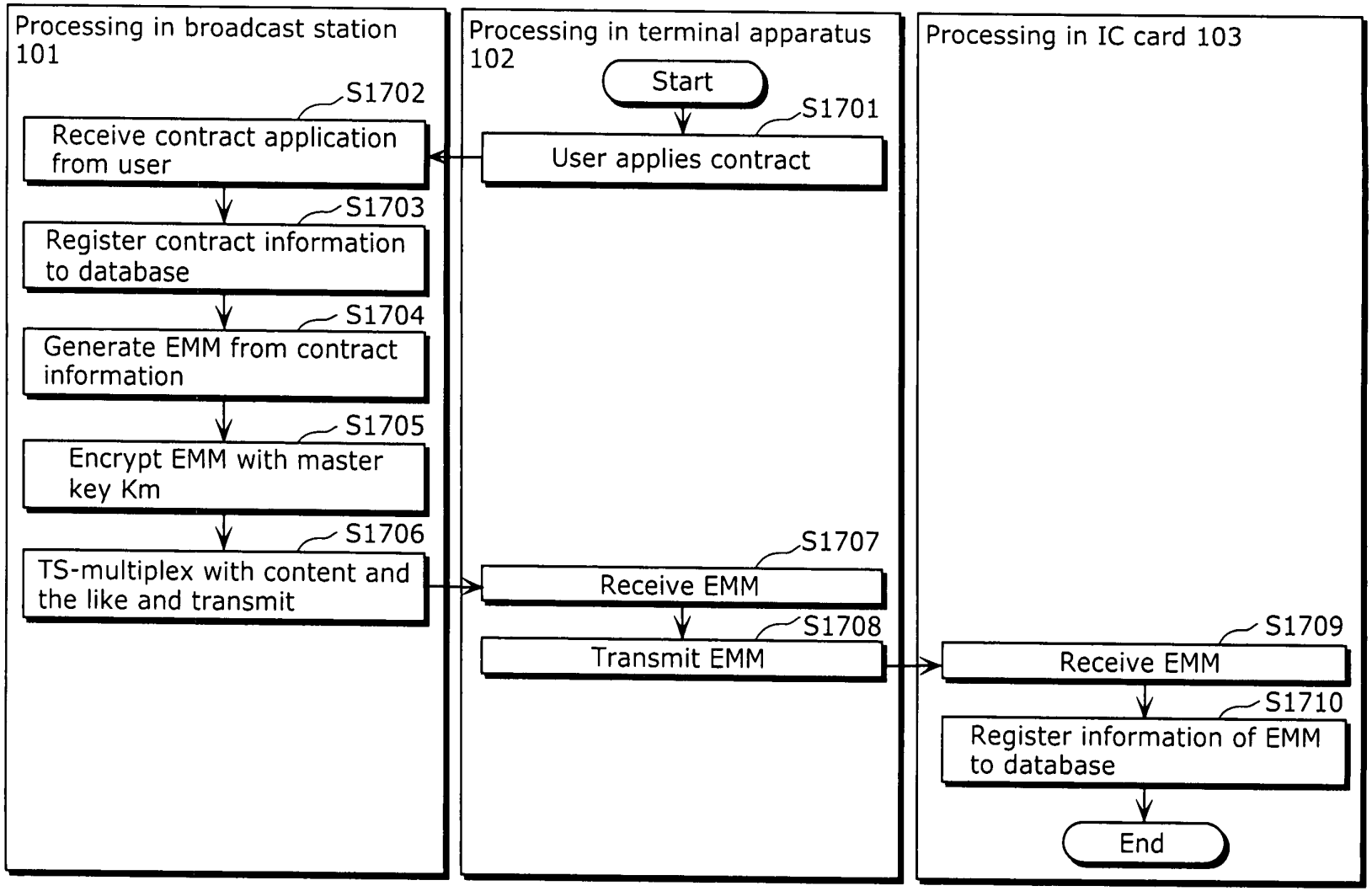

Processing in broadcast station 101
Processing in terminal apparatus 102
Processing in IC card 103
Start
S1701
User applies contract
S1702
Receive contract application from user
S1703
Register contract information to database
S1704
Generate EMM from contract information
S1705
Encrypt EMM with master key Km
S1706
TS-multiplex with content and the like and transmit
S1707
Receive EMM
S1708
Transmit EMM
S1709
Receive EMM
S1710
Register information of EMM to database
End

FIG. 18

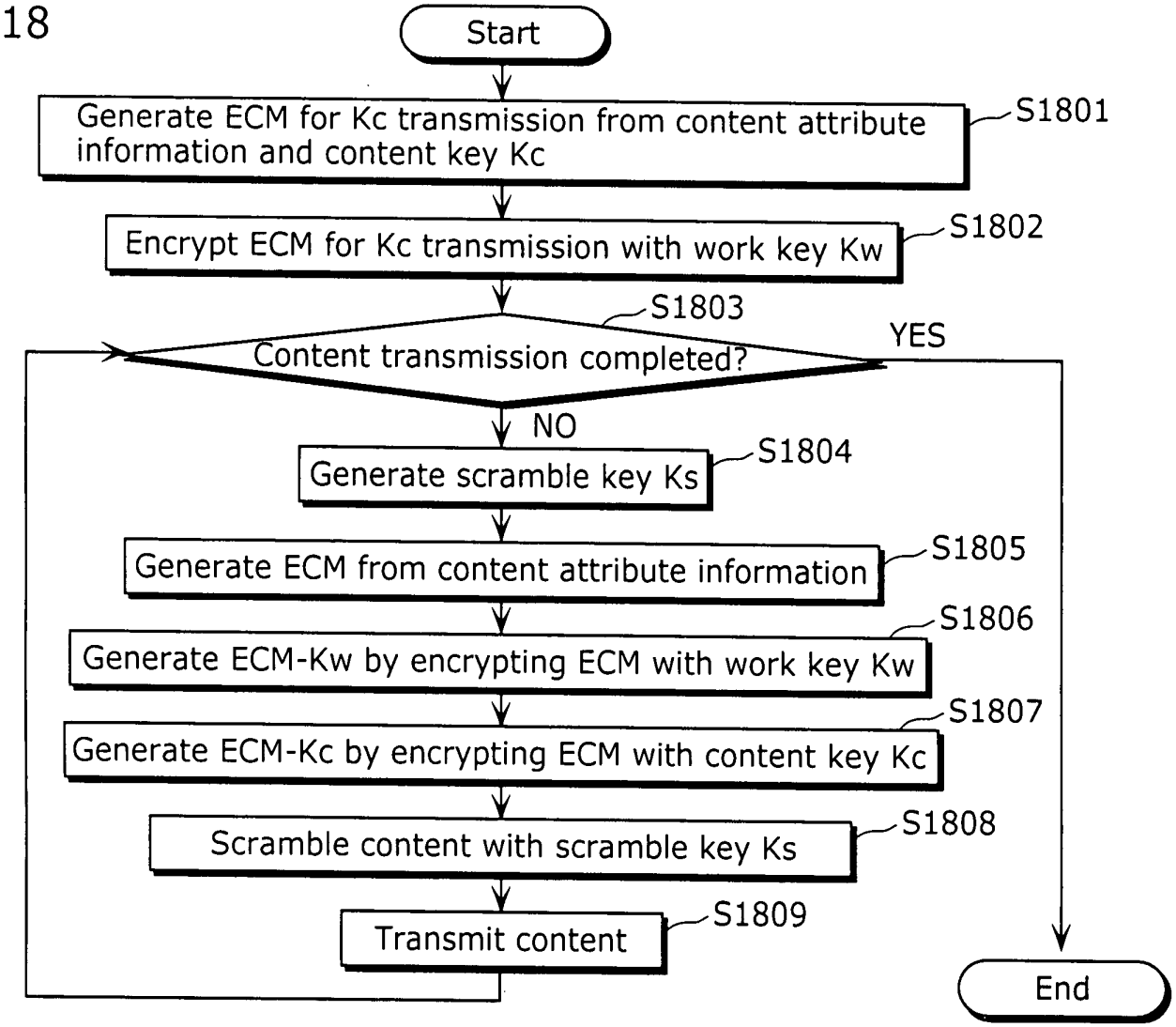

Start
Generate ECM for Kc transmission from content attribute information and content key Kc
S1801
Encrypt ECM for Kc transmission with work key Kw
S1802
S1803
Content transmission completed?
YES
NO
Generate scramble key Ks
S1804
Generate ECM from content attribute information
S1805
Generate ECM-Kw by encrypting ECM with work key Kw
S1806
Generate ECM-Kc by encrypting ECM with content key Kc
S1807
Scramble content with scramble key Ks
S1808
Transmit content
S1809
End

FIG. 19

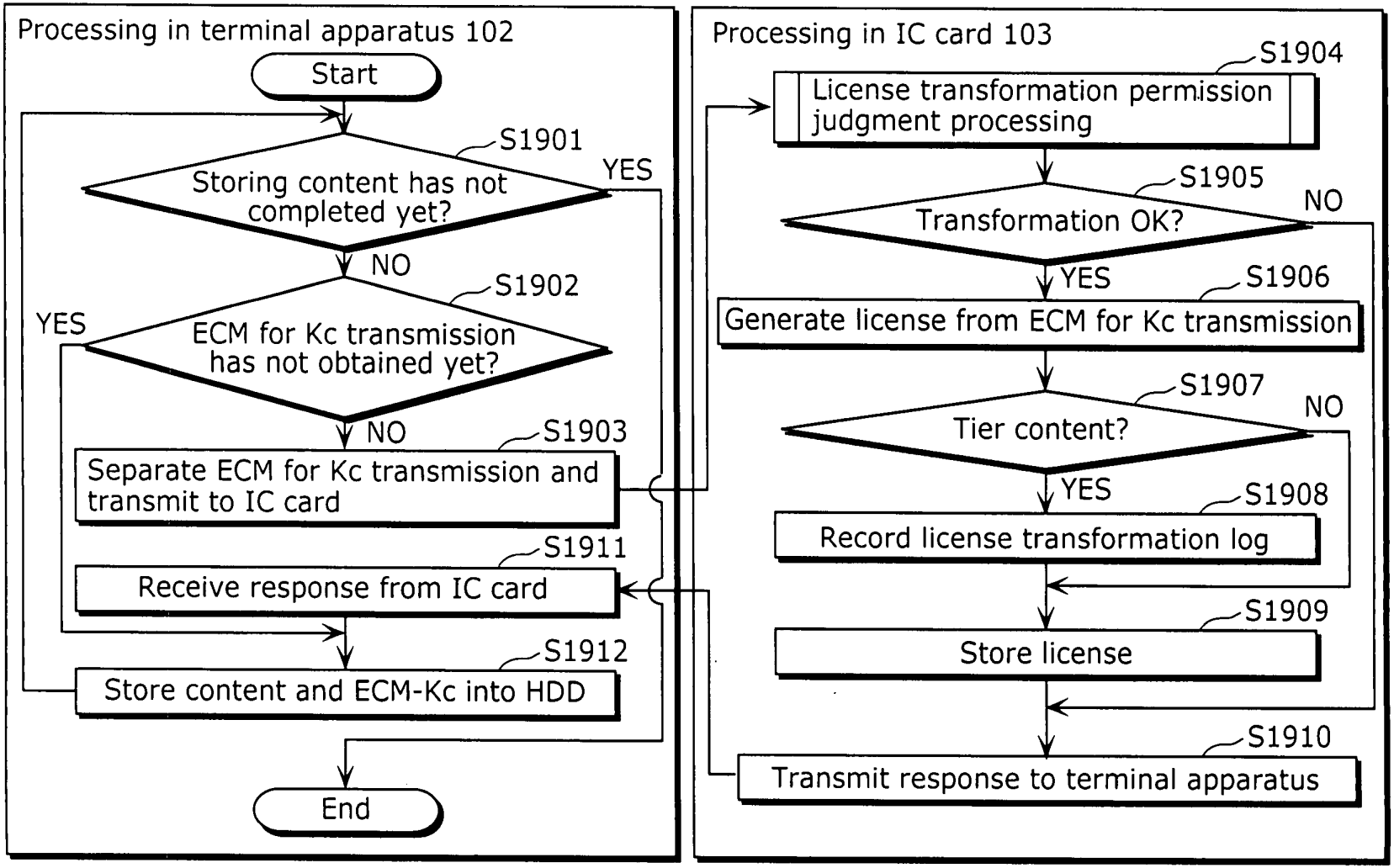

Processing in terminal apparatus 102
Start
S1901
Storing content has not completed yet?
YES
NO
S1902
ECM for Kc transmission has not obtained yet?
YES
NO
S1903
Separate ECM for Kc transmission and transmit to IC card
S1911
Receive response from IC card
S1912
Store content and ECM-Kc into HDD
End
Processing in IC card 103
S1904
License transformation permission judgment processing
S1905
Transformation OK?
NO
YES
S1906
Generate license from ECM for Kc transmission
S1907
Tier content?
NO
YES
S1908
Record license transformation log
S1909
Store license
S1910
Transmit response to terminal apparatus

FIG. 20

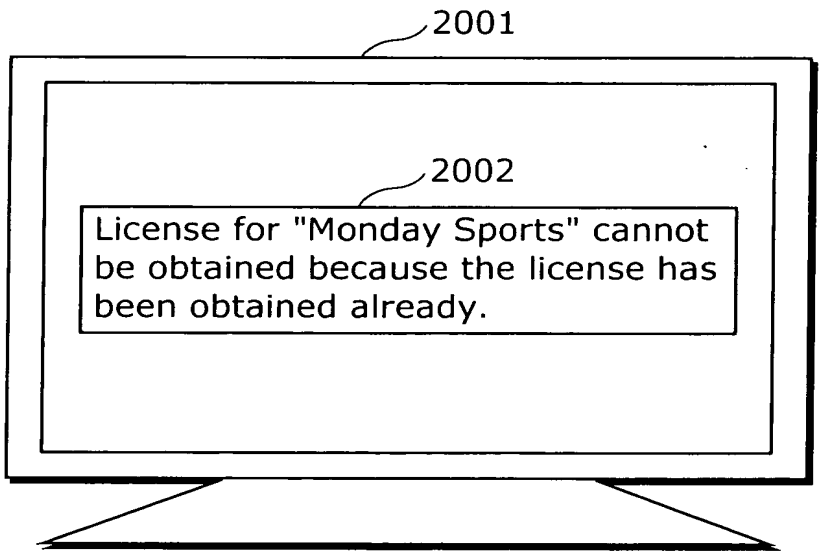

2001
2002
License for "Monday Sports" cannot be obtained because the license has been obtained already.

FIG. 21

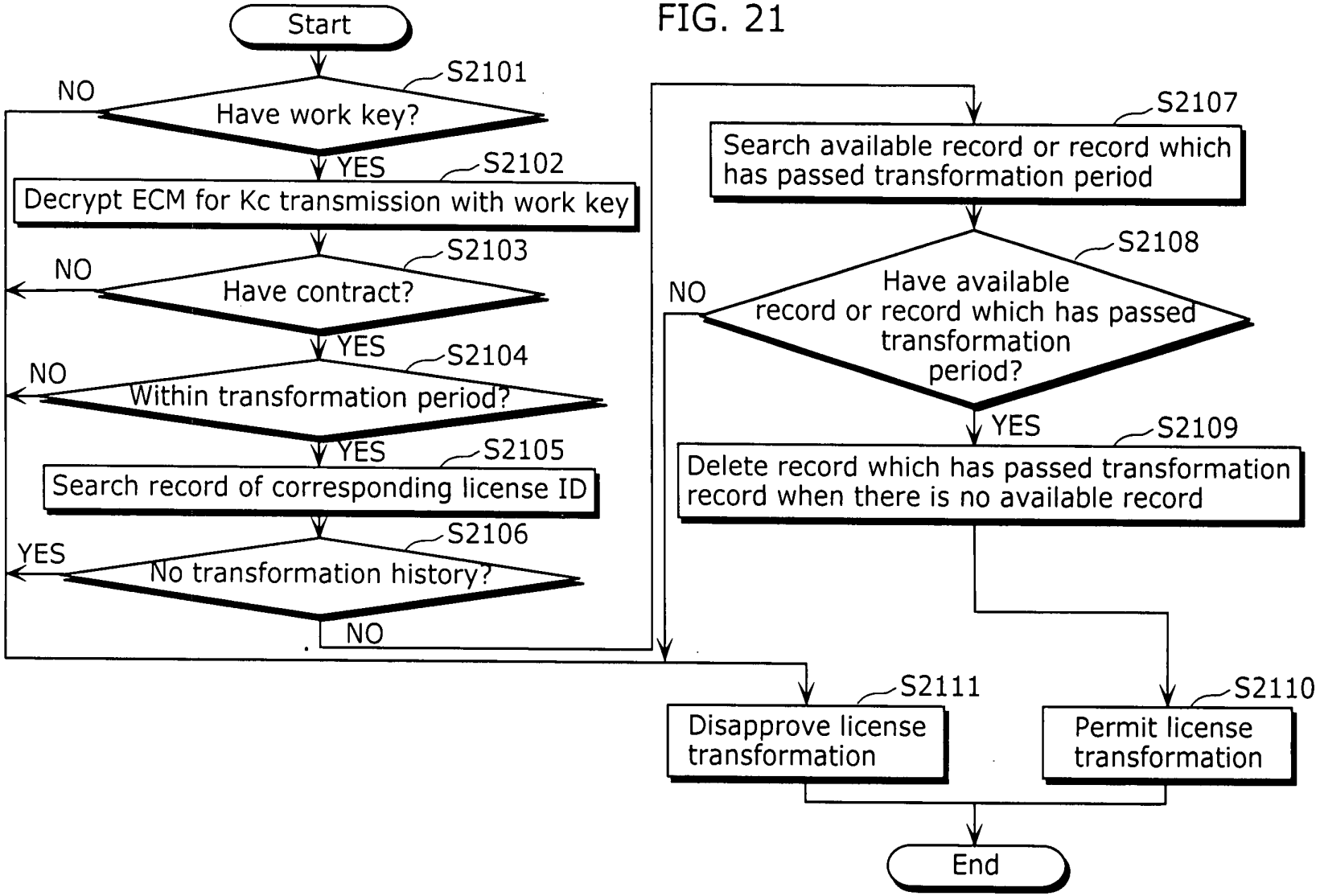

Start
S2101
Have work key?
NO
YES
S2102
Decrypt ECM for Kc transmission with work key
S2103
Have contract?
NO
YES
S2104
Within transformation period?
NO
YES
S2105
Search record of corresponding license ID
S2106
No transformation history?
YES
NO
S2107
Search available record or record which has passed transformation period
S2108
Have available record or record which has passed transformation period?
NO
YES
S2109
Delete record which has passed transformation record when there is no available record
S2111
Disapprove license transformation
S2110
Permit license transformation
End

FIG. 22

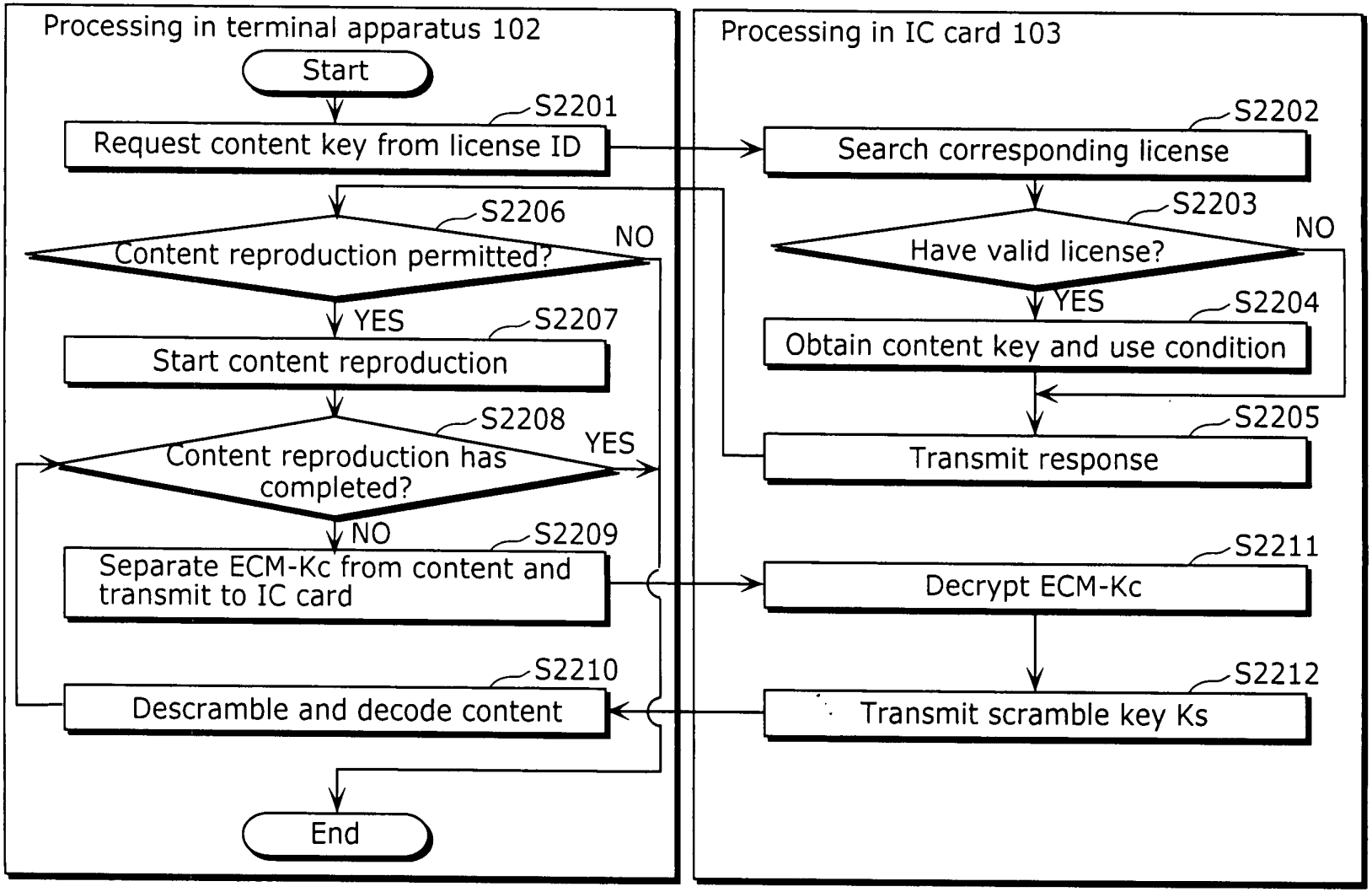

Processing in terminal apparatus 102
Start
S2201
Request content key from license ID
S2206
Content reproduction permitted?
NO
YES
S2207
Start content reproduction
S2208
Content reproduction has completed?
YES
NO
S2209
Separate ECM-Kc from content and transmit to IC card
S2210
Descramble and decode content
End
Processing in IC card 103
S2202
Search corresponding license
S2203
Have valid license?
NO
YES
S2204
Obtain content key and use condition
S2205
Transmit response
S2211
Decrypt ECM-Kc
S2212
Transmit scramble key Ks

FIG. 23

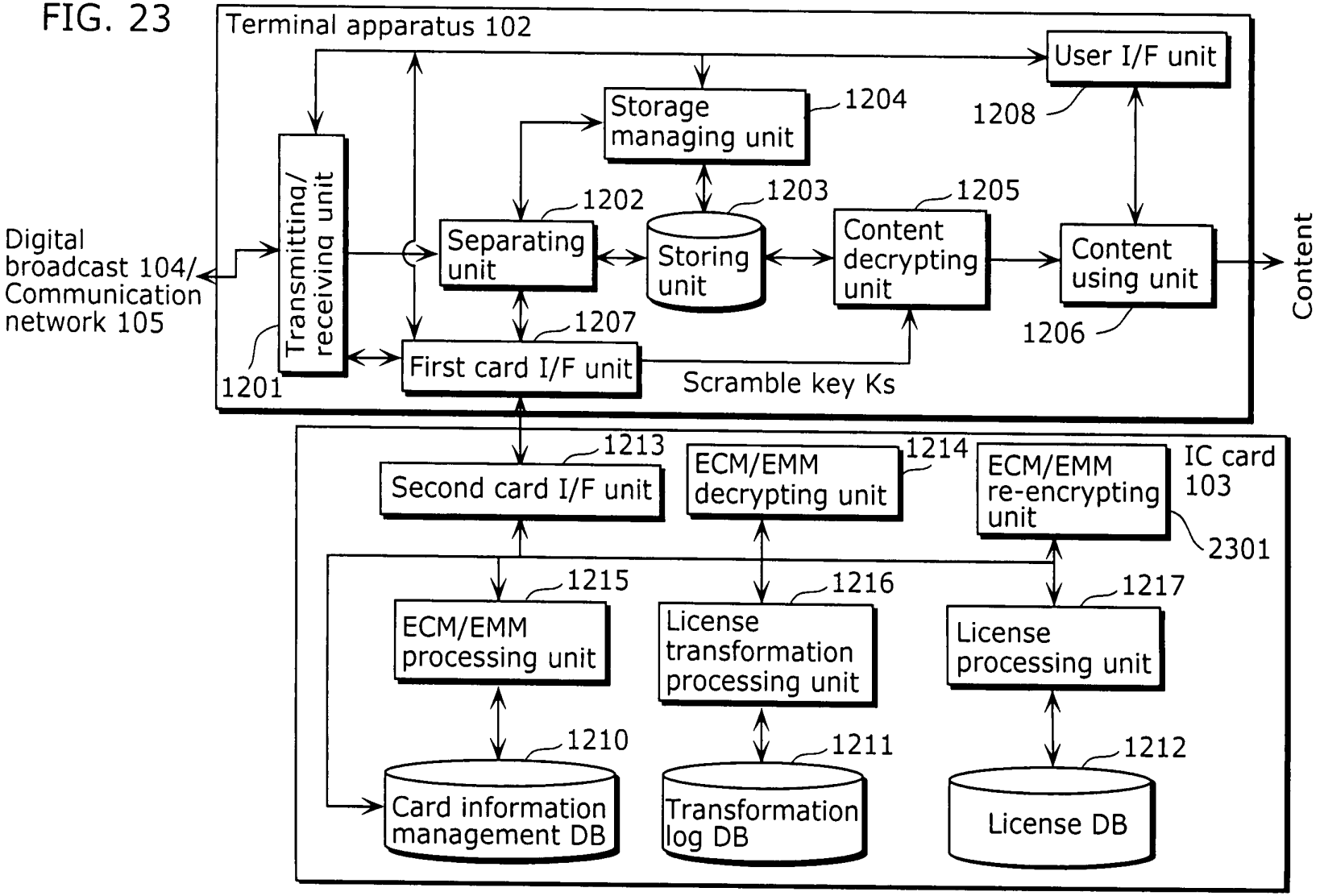

Terminal apparatus 102
User I/F unit
1208
Storage managing unit
1204
1202
1203
1205
Digital broadcast 104/ Communication network 105
Transmitting/ receiving unit
Separating unit
Storing unit
Content decrypting unit
Content using unit
Content
1207
1206
1201
First card I/F unit
Scramble key Ks
1213
1214
IC card 103
Second card I/F unit
ECM/EMM decrypting unit
ECM/EMM re-encrypting unit
2301
1215
1216
1217
ECM/EMM processing unit
License transformation processing unit
License processing unit
1210
1211
1212
Card information management DB
Transformation log DB
License DB

FIG. 24

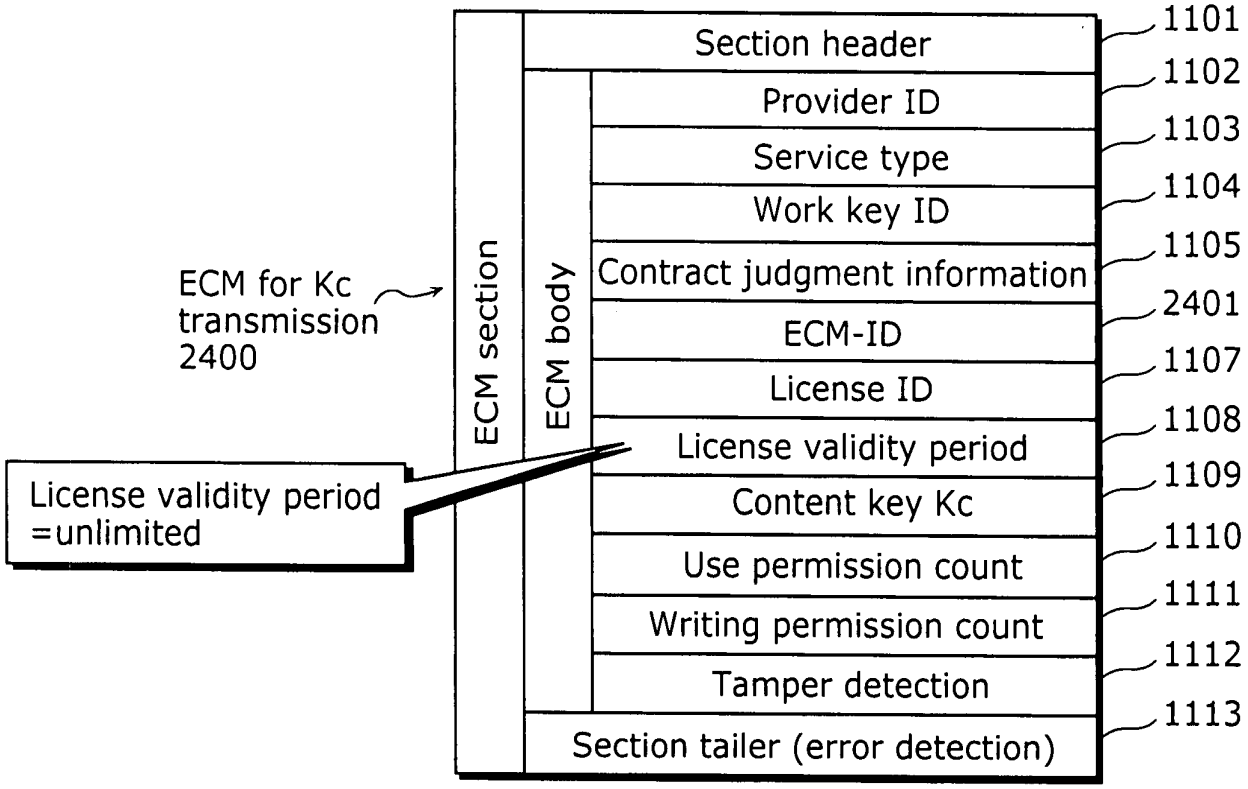

ECM for Kc transmission 2400
License validity period =unlimited
ECM section
ECM body
Section header
Provider ID
Service type
Work key ID
Contract judgment information
ECM-ID
License ID
License validity period
Content key Kc
Use permission count
Writing permission count
Tamper detection
Section tailer (error detection)
1101
1102
1103
1104
1105
2401
1107
1108
1109
1110
1111
1112
1113

FIG. 25

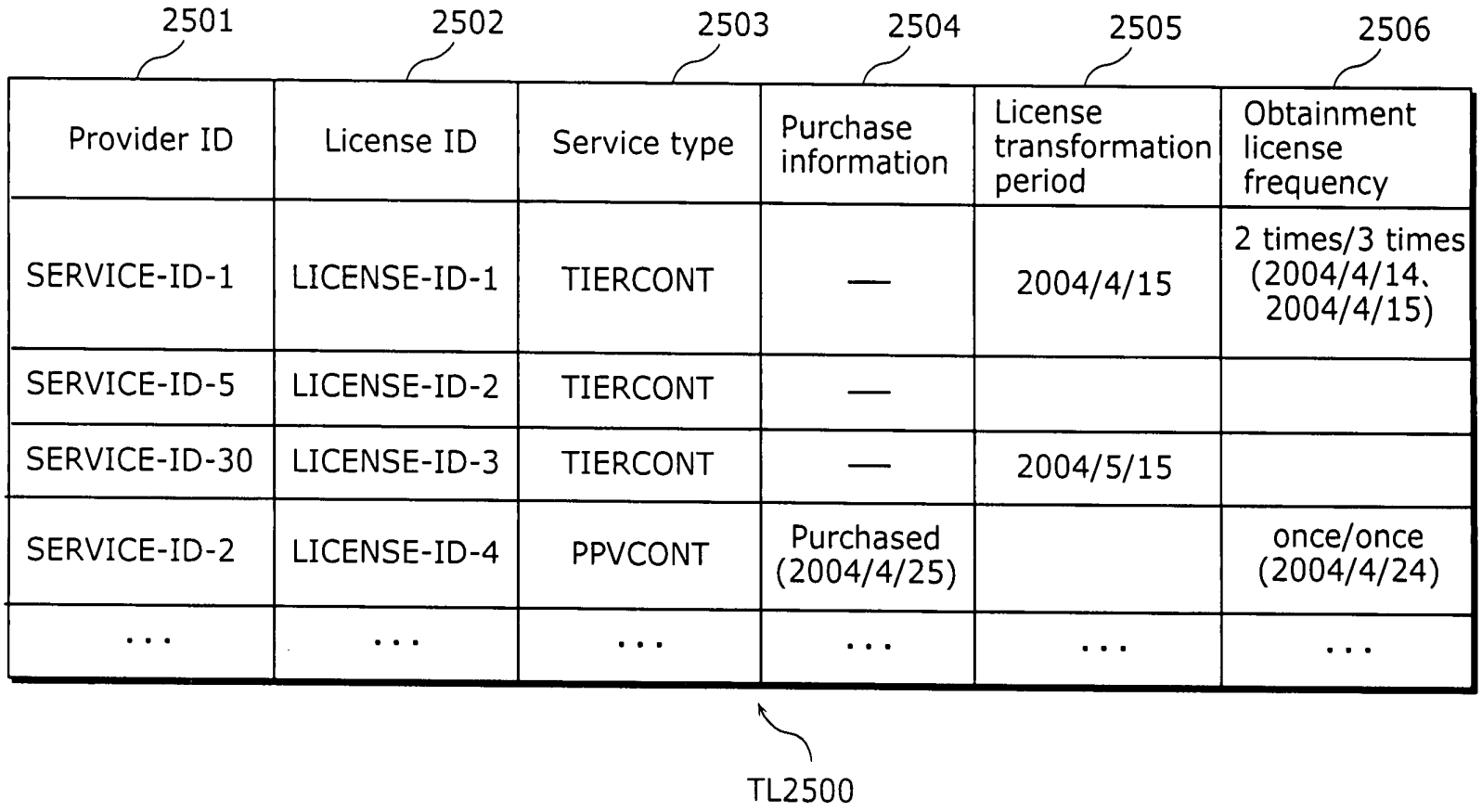

2501
2502
2503
2504
2505
2506
Provider ID
License ID
Service type
Purchase information
License transformation period
Obtainment license frequency
SERVICE-ID-1
LICENSE-ID-1
TIERCONT
—
2004/4/15
2 times/3 times (2004/4/14, 2004/4/15)
SERVICE-ID-5
LICENSE-ID-2
TIERCONT
—
SERVICE-ID-30
LICENSE-ID-3
TIERCONT
—
2004/5/15
SERVICE-ID-2
LICENSE-ID-4
PPVCONT
Purchased (2004/4/25)
once/once (2004/4/24)
TL2500

FIG. 26

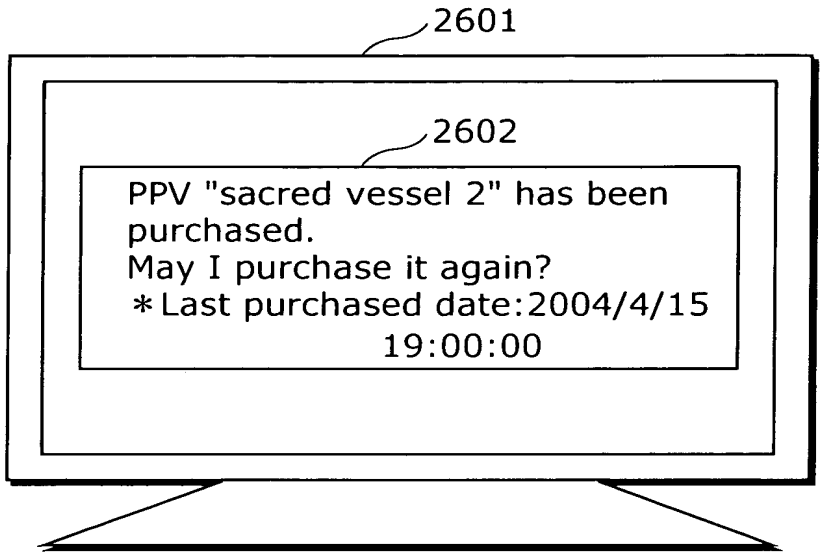

2601
2602
PPV "sacred vessel 2" has been purchased.
May I purchase it again?
*Last purchased date:2004/4/15 19:00:00

FIG. 27

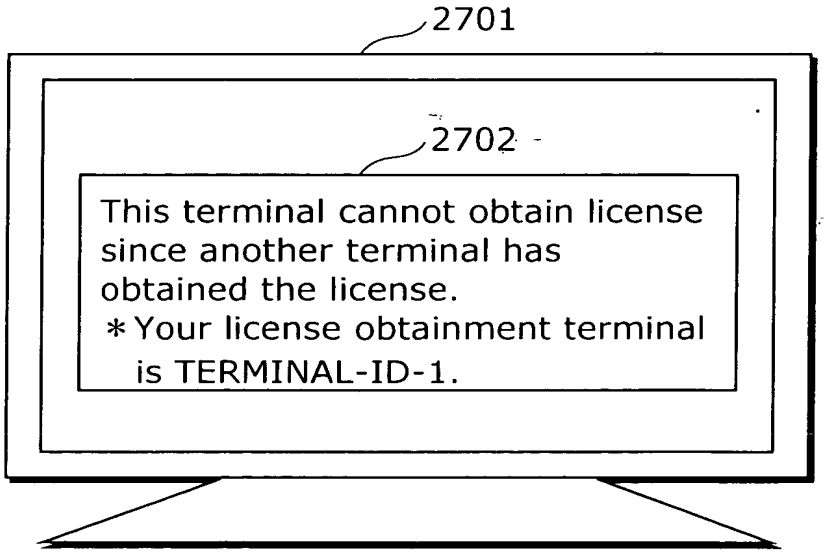

2701
2702
This terminal cannot obtain license since another terminal has obtained the license.
*Your license obtainment terminal is TERMINAL-ID-1.

FIG. 28

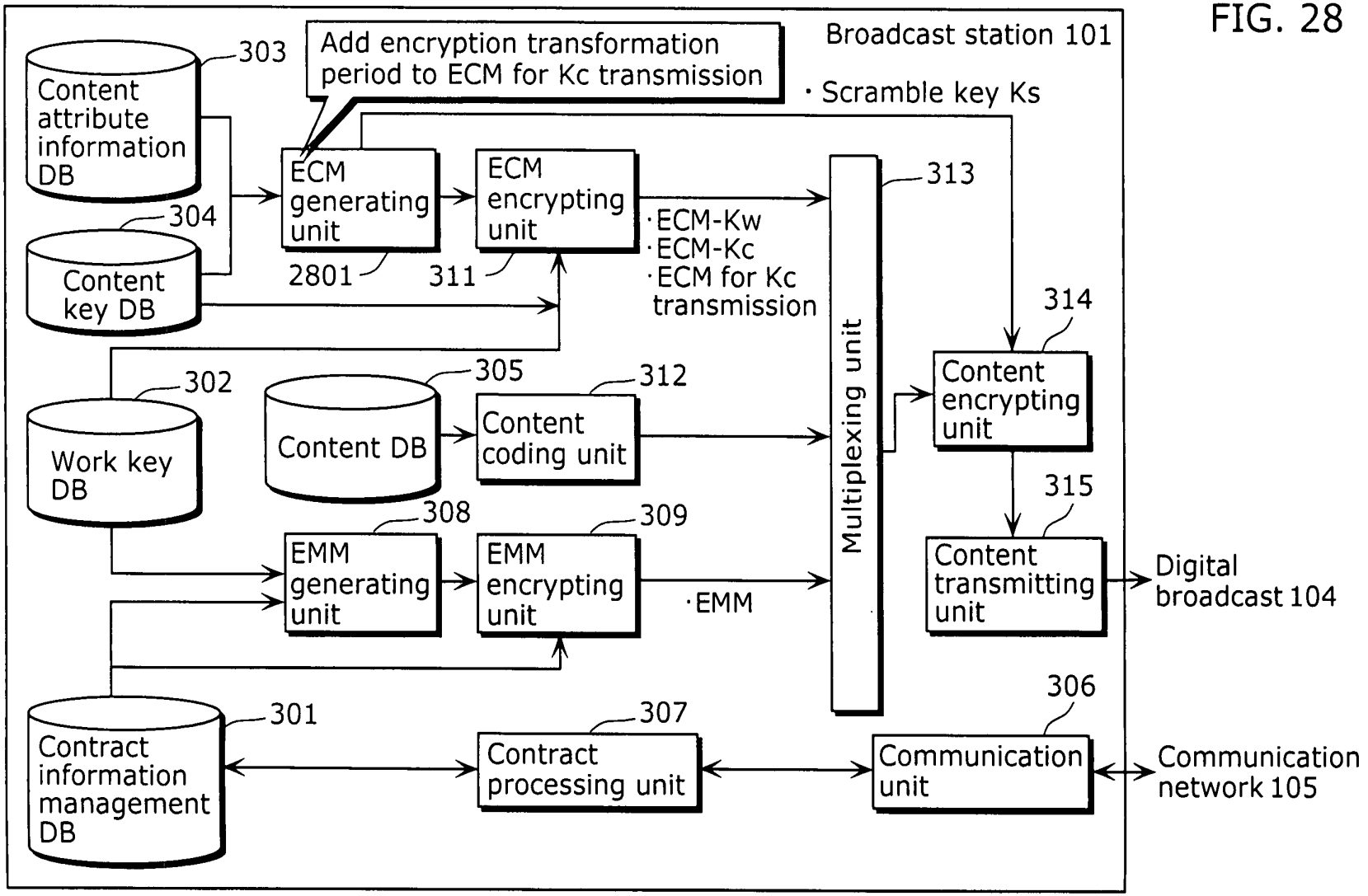

Broadcast station 101
Add encryption transformation period to ECM for Kc transmission
· Scramble key Ks
303
Content attribute information DB
304
Content key DB
ECM generating unit
2801
ECM encrypting unit
311
·ECM-Kw
·ECM-Kc
·ECM for Kc transmission
313
Multiplexing unit
314
Content encrypting unit
315
Content transmitting unit
Digital broadcast 104
302
Work key DB
305
Content DB
312
Content coding unit
308
EMM generating unit
309
EMM encrypting unit
·EMM
301
Contract information management DB
307
Contract processing unit
306
Communication unit
Communication network 105

FIG. 29

2901 Content ID	2902 License ID	2903 Use condition	2904 Contract information	2905 Encryption transformation period
CONTENT-ID-1	LICENSE-ID-1	Validity period: 1 month	TIERCONT-ID-1	2004/4/15
CONTENT-ID-2	LICENSE-ID-2	Validity period: 1 month. Reproduction count: 10 times	TIERCONT-ID-1 TIERCONT-ID-2	2004/4/18
CONTENT-ID-3	LICENSE-ID-3	Validity period: 3 months	TIERCONT-ID-1	2004/4/17
CONTENT-ID-4	LICENSE-ID-4	Validity period: 3 days. Writing count: once	PPVCONT-ID-1	2004/5/14
...	...	...		...

Content attribute information management table 2900

FIG. 30

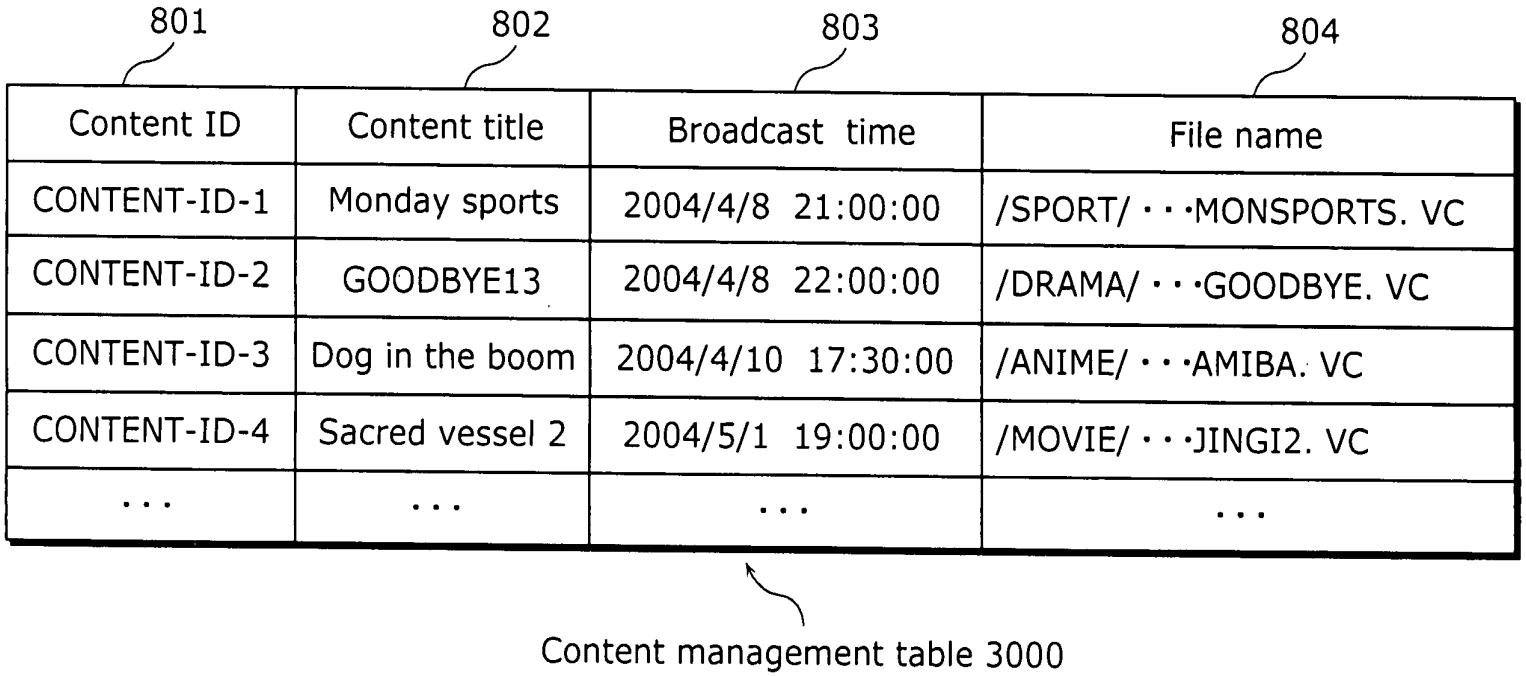

801
802
803
804
Content ID
Content title
Broadcast time
File name
CONTENT-ID-1
Monday sports
2004/4/8 21:00:00
/SPORT/・・・MONSPORTS. VC
CONTENT-ID-2
GOODBYE13
2004/4/8 22:00:00
/DRAMA/・・・GOODBYE. VC
CONTENT-ID-3
Dog in the boom
2004/4/10 17:30:00
/ANIME/・・・AMIBA. VC
CONTENT-ID-4
Sacred vessel 2
2004/5/1 19:00:00
/MOVIE/・・・JINGI2. VC
・・・
・・・
・・・
・・・
Content management table 3000

FIG. 31

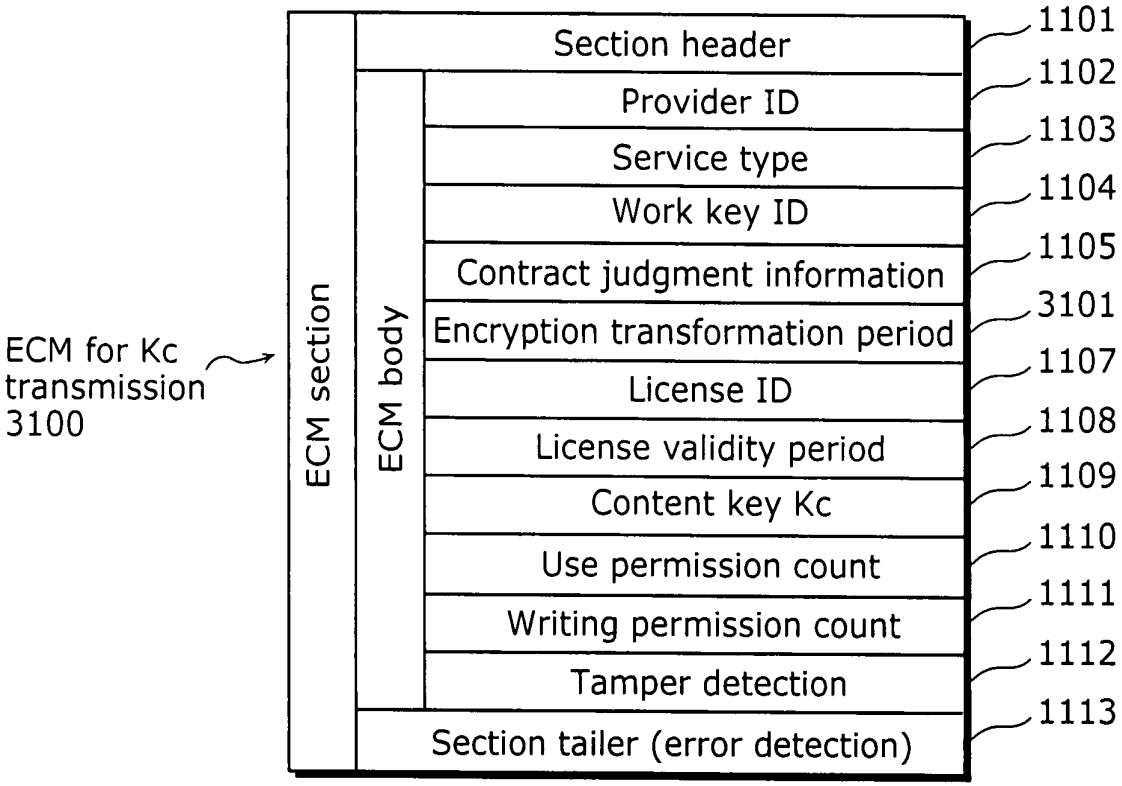

ECM for Kc transmission 3100
ECM section
ECM body
Section header
Provider ID
Service type
Work key ID
Contract judgment information
Encryption transformation period
License ID
License validity period
Content key Kc
Use permission count
Writing permission count
Tamper detection
Section tailer (error detection)
1101
1102
1103
1104
1105
3101
1107
1108
1109
1110
1111
1112
1113

FIG. 32

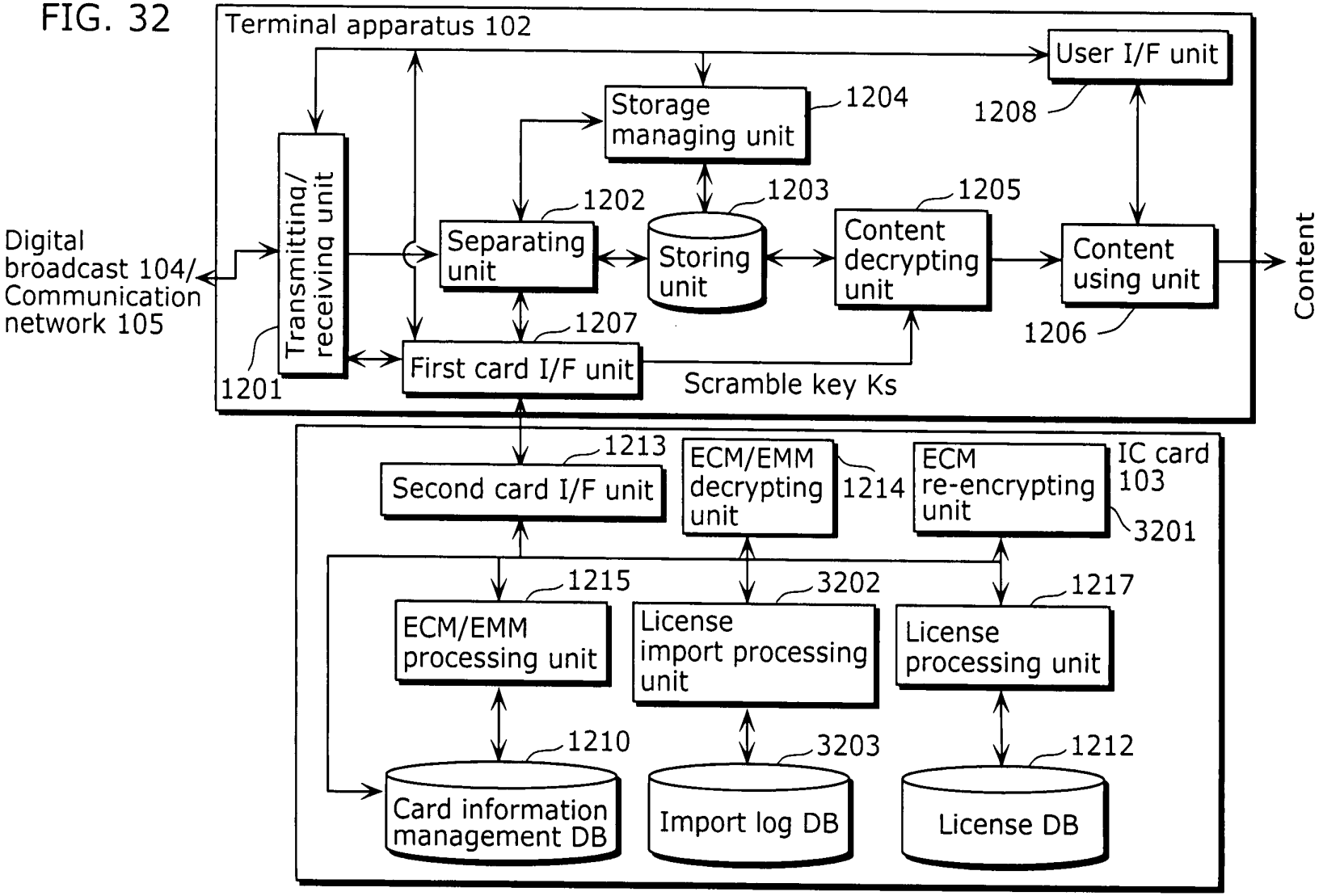

Terminal apparatus 102
User I/F unit
1208
Storage managing unit
1204
Transmitting/ receiving unit
1202
1203
1205
Digital broadcast 104/ Communication network 105
Separating unit
Storing unit
Content decrypting unit
Content using unit
Content
1207
1206
1201
First card I/F unit
Scramble key Ks
1213
ECM/EMM decrypting unit
1214
ECM re-encrypting unit
IC card 103
3201
Second card I/F unit
1215
3202
1217
ECM/EMM processing unit
License import processing unit
License processing unit
1210
3203
1212
Card information management DB
Import log DB
License DB

FIG. 33

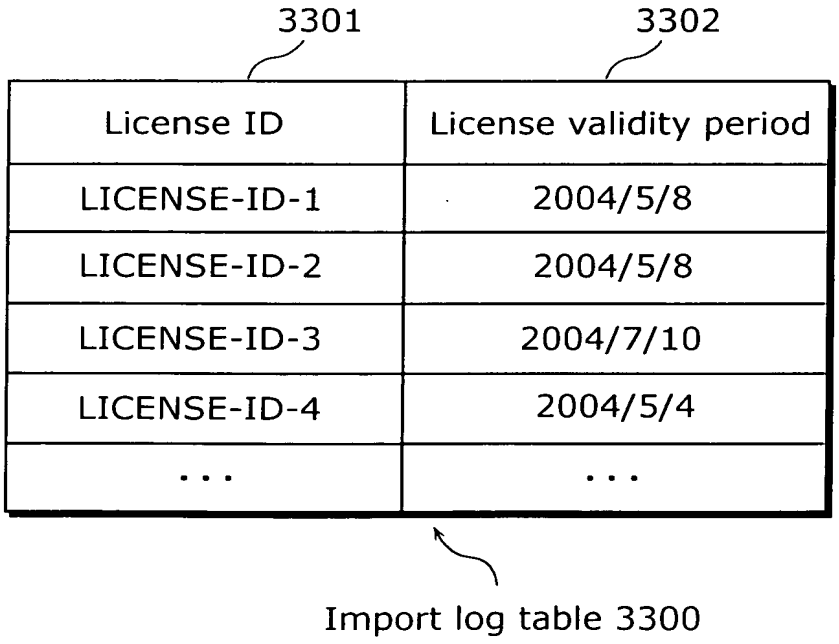

3301
3302
License ID
License validity period
LICENSE-ID-1
2004/5/8
LICENSE-ID-2
2004/5/8
LICENSE-ID-3
2004/7/10
LICENSE-ID-4
2004/5/4
...
...
Import log table 3300

FIG. 34

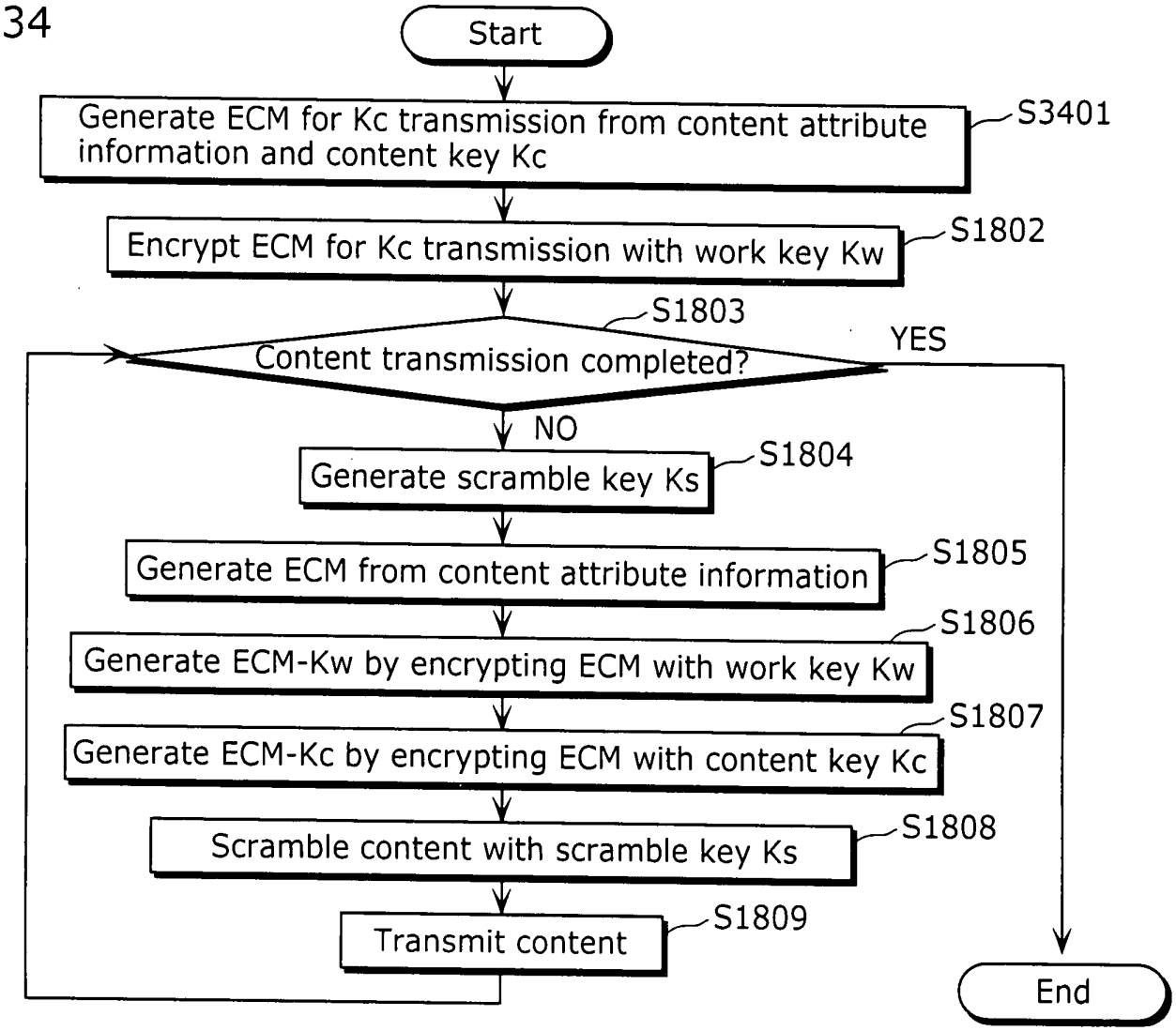

Start
Generate ECM for Kc transmission from content attribute information and content key Kc
S3401
Encrypt ECM for Kc transmission with work key Kw
S1802
S1803
Content transmission completed?
YES
NO
Generate scramble key Ks
S1804
Generate ECM from content attribute information
S1805
Generate ECM-Kw by encrypting ECM with work key Kw
S1806
Generate ECM-Kc by encrypting ECM with content key Kc
S1807
Scramble content with scramble key Ks
S1808
Transmit content
S1809
End

FIG. 35

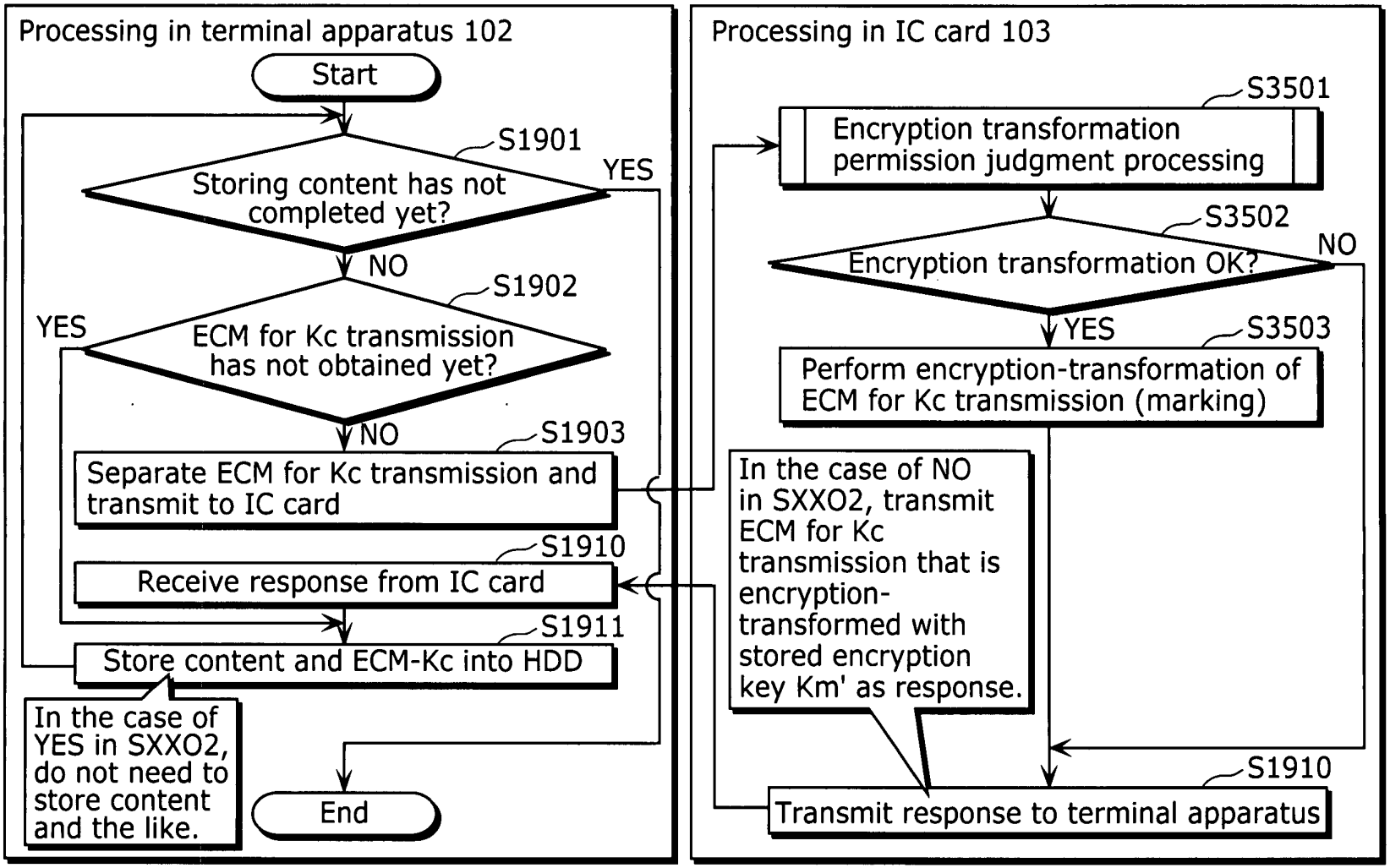

Processing in terminal apparatus 102
Start
S1901
Storing content has not completed yet?
YES
NO
S1902
ECM for Kc transmission has not obtained yet?
YES
NO
S1903
Separate ECM for Kc transmission and transmit to IC card
S1910
Receive response from IC card
S1911
Store content and ECM-Kc into HDD
In the case of YES in SXXO2, do not need to store content and the like.
End
Processing in IC card 103
S3501
Encryption transformation permission judgment processing
S3502
Encryption transformation OK?
NO
YES
S3503
Perform encryption-transformation of ECM for Kc transmission (marking)
In the case of NO in SXXO2, transmit ECM for Kc transmission that is encryption-transformed with stored encryption key Km' as response.
S1910
Transmit response to terminal apparatus

FIG. 36

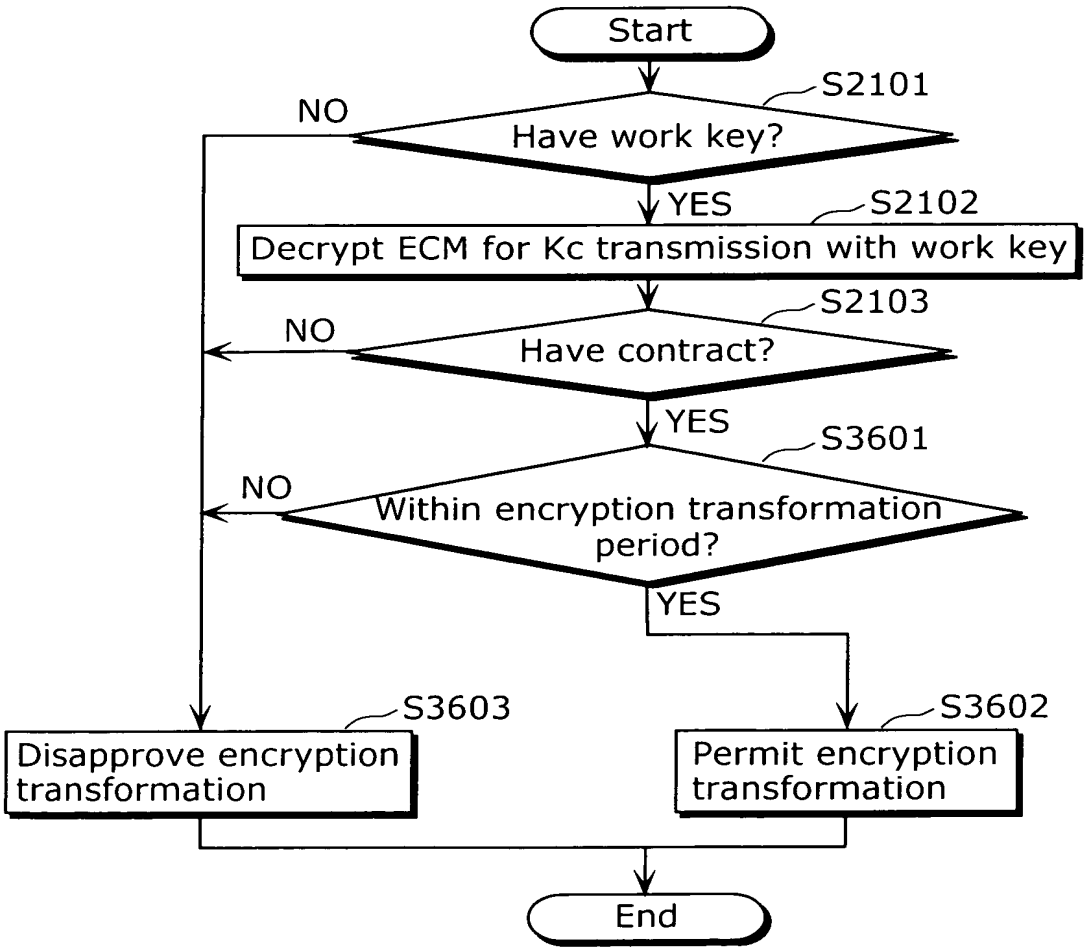

Start
S2101
NO
Have work key?
YES
S2102
Decrypt ECM for Kc transmission with work key
S2103
NO
Have contract?
YES
S3601
NO
Within encryption transformation period?
YES
S3603
Disapprove encryption transformation
S3602
Permit encryption transformation
End

FIG. 37

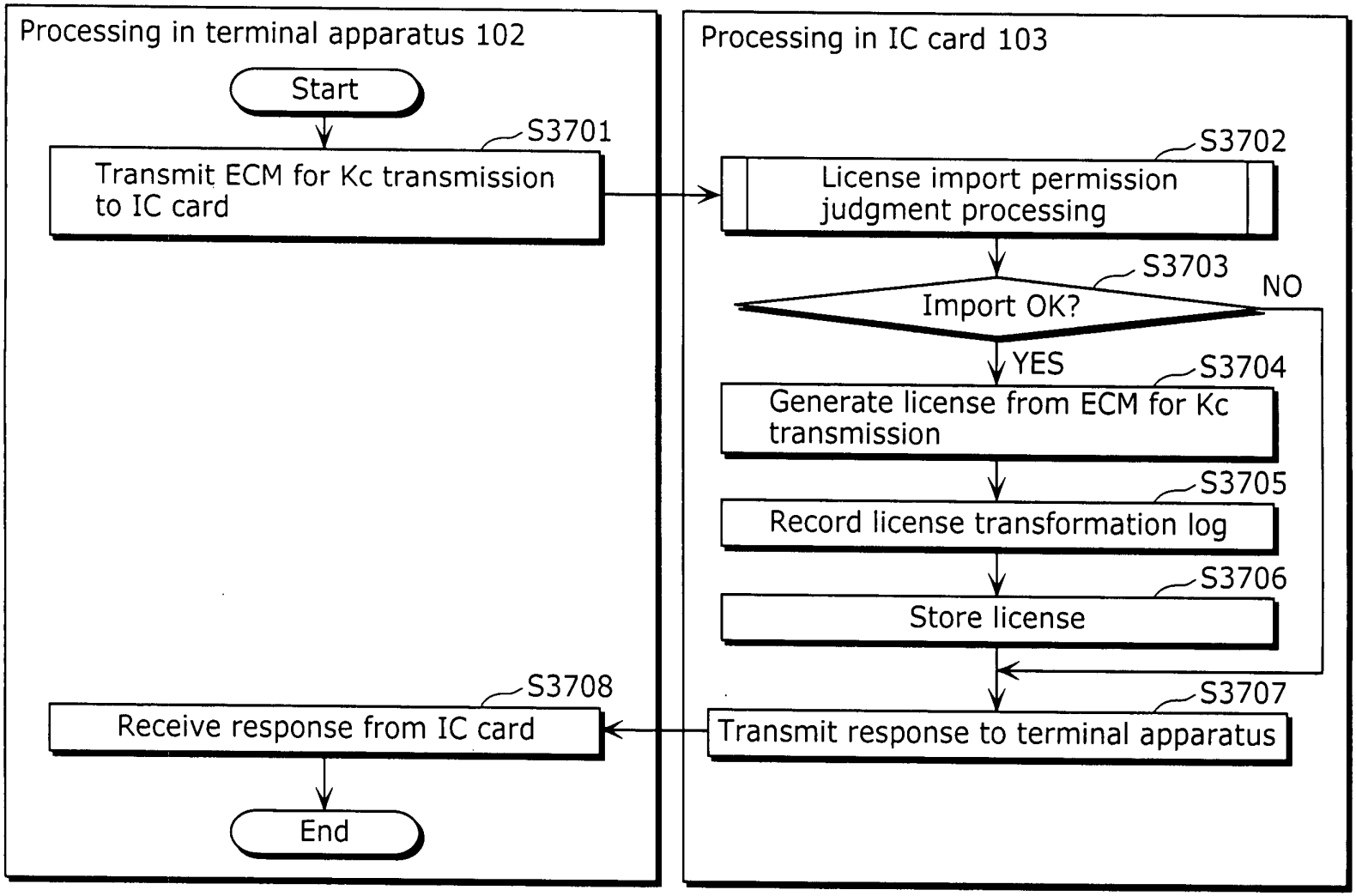

Processing in terminal apparatus 102
Start
S3701
Transmit ECM for Kc transmission to IC card
S3708
Receive response from IC card
End
Processing in IC card 103
S3702
License import permission judgment processing
S3703
Import OK?
NO
YES
S3704
Generate license from ECM for Kc transmission
S3705
Record license transformation log
S3706
Store license
S3707
Transmit response to terminal apparatus

FIG. 38

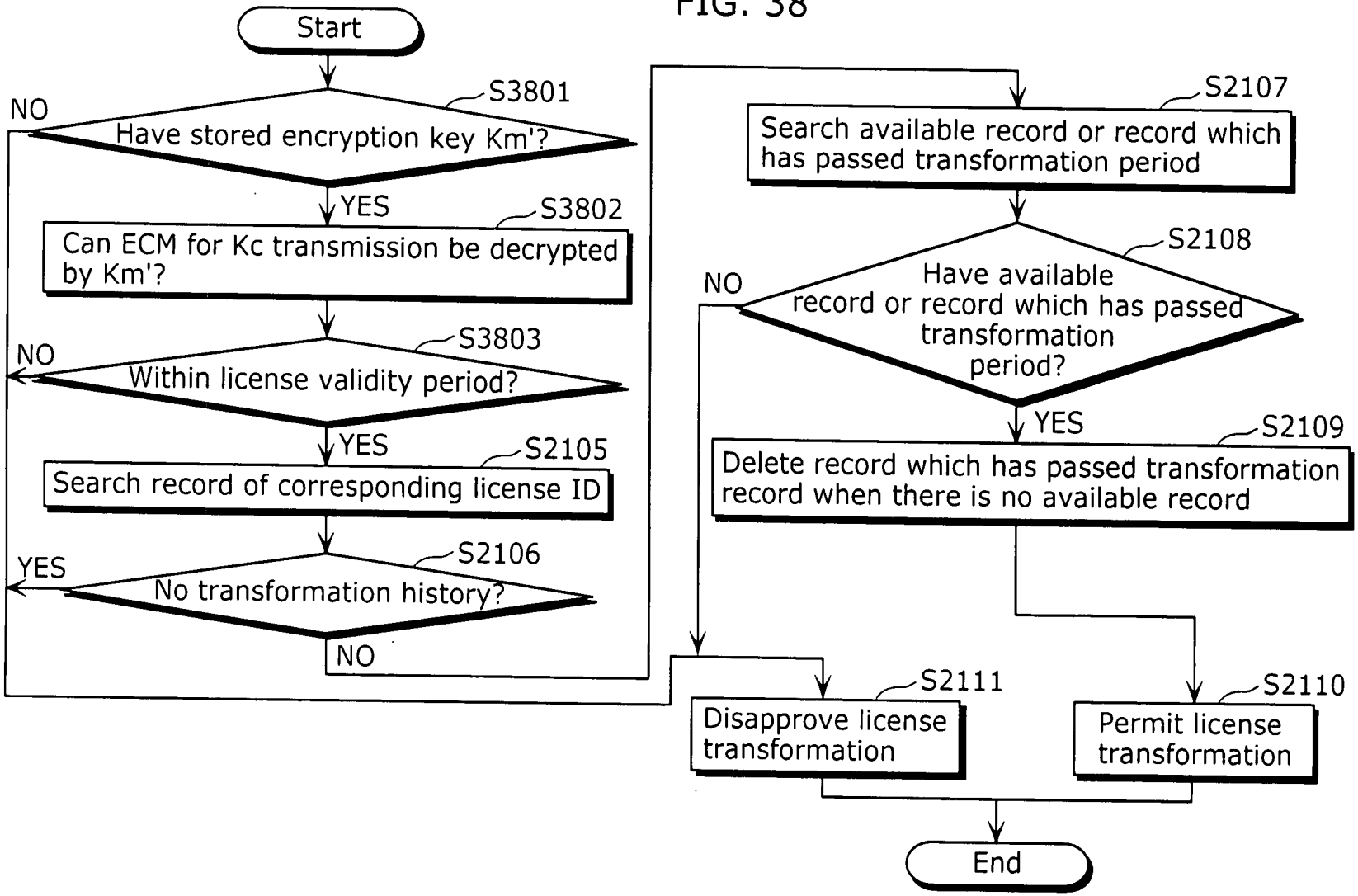

Start
S3801
Have stored encryption key Km'?
NO
YES
S3802
Can ECM for Kc transmission be decrypted by Km'?
S3803
Within license validity period?
NO
YES
S2105
Search record of corresponding license ID
S2106
No transformation history?
YES
NO
S2107
Search available record or record which has passed transformation period
S2108
Have available record or record which has passed transformation period?
NO
YES
S2109
Delete record which has passed transformation record when there is no available record
S2111
Disapprove license transformation
S2110
Permit license transformation
End

FIG. 39

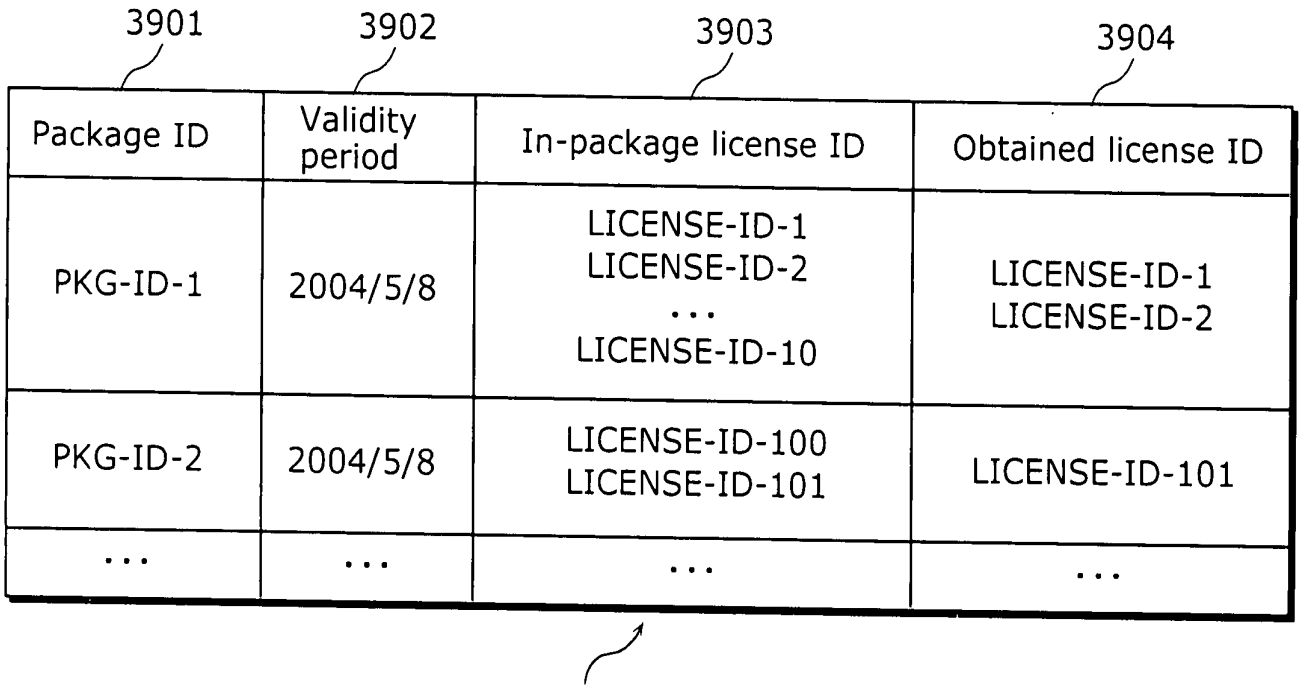

3901
3902
3903
3904
Package ID
Validity period
In-package license ID
Obtained license ID
PKG-ID-1
2004/5/8
LICENSE-ID-1
LICENSE-ID-2
...
LICENSE-ID-10
LICENSE-ID-1
LICENSE-ID-2
PKG-ID-2
2004/5/8
LICENSE-ID-100
LICENSE-ID-101
LICENSE-ID-101
...
...
...
...
Import log table (IL: Import List) 3900

FIG. 40

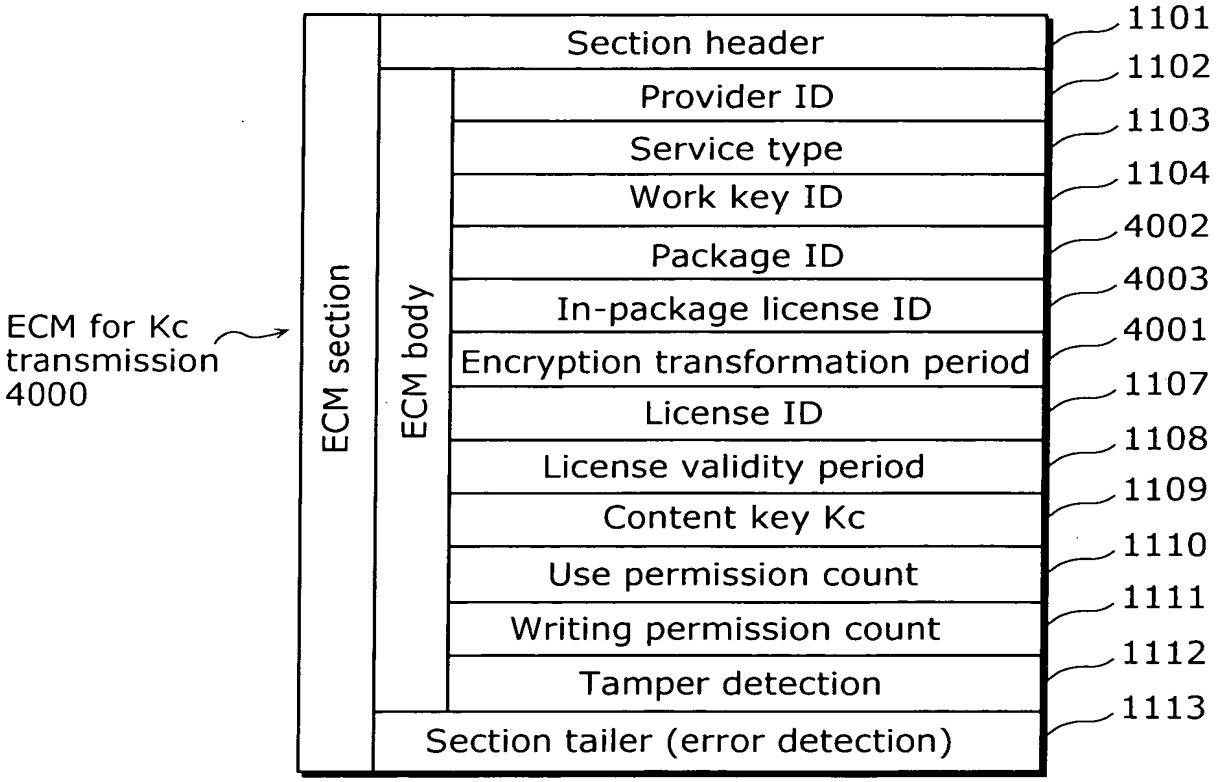

ECM for Kc transmission 4000
ECM section
ECM body
Section header
Provider ID
Service type
Work key ID
Package ID
In-package license ID
Encryption transformation period
License ID
License validity period
Content key Kc
Use permission count
Writing permission count
Tamper detection
Section tailer (error detection)
1101
1102
1103
1104
4002
4003
4001
1107
1108
1109
1110
1111
1112
1113

FIG. 41

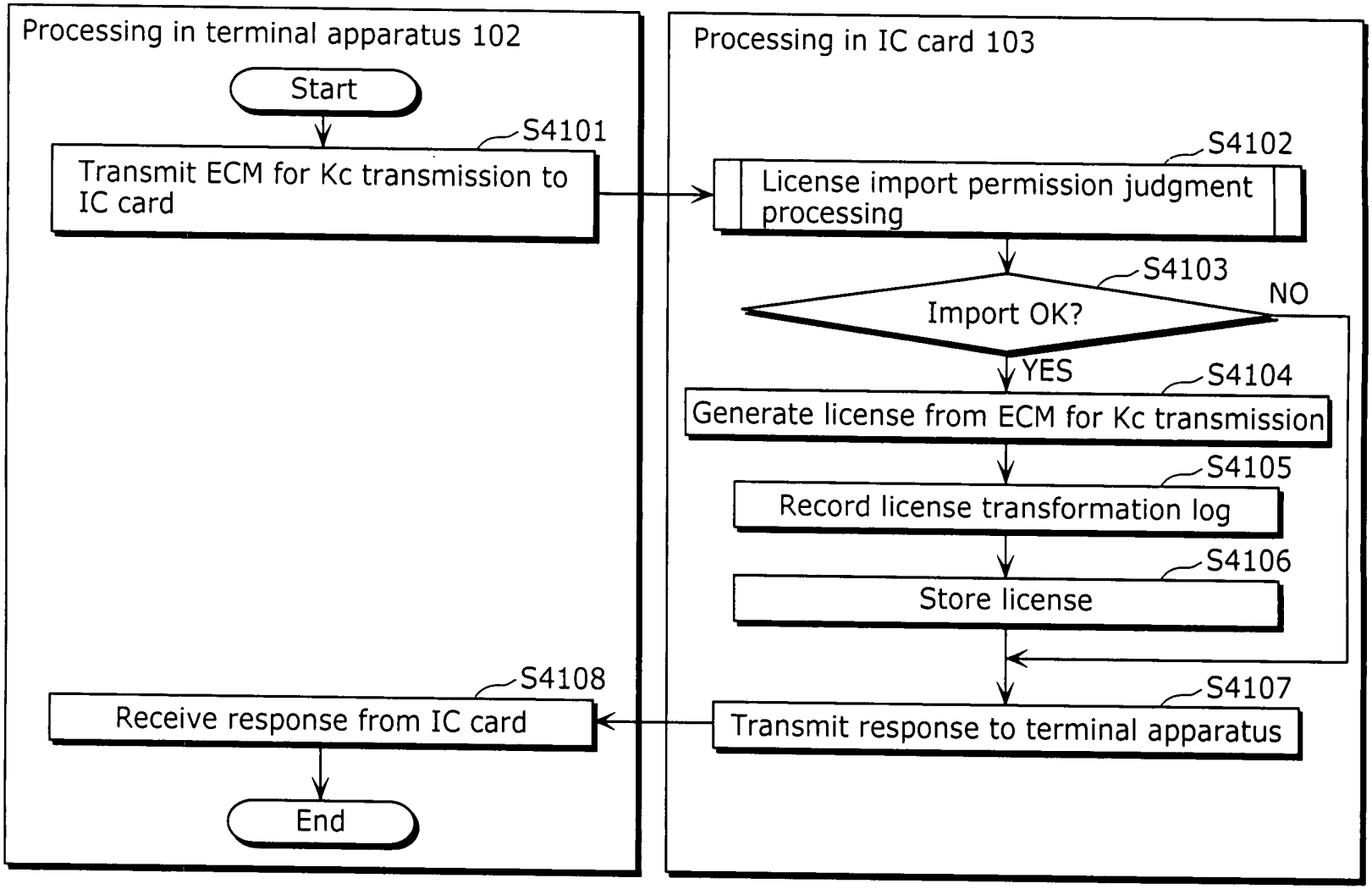
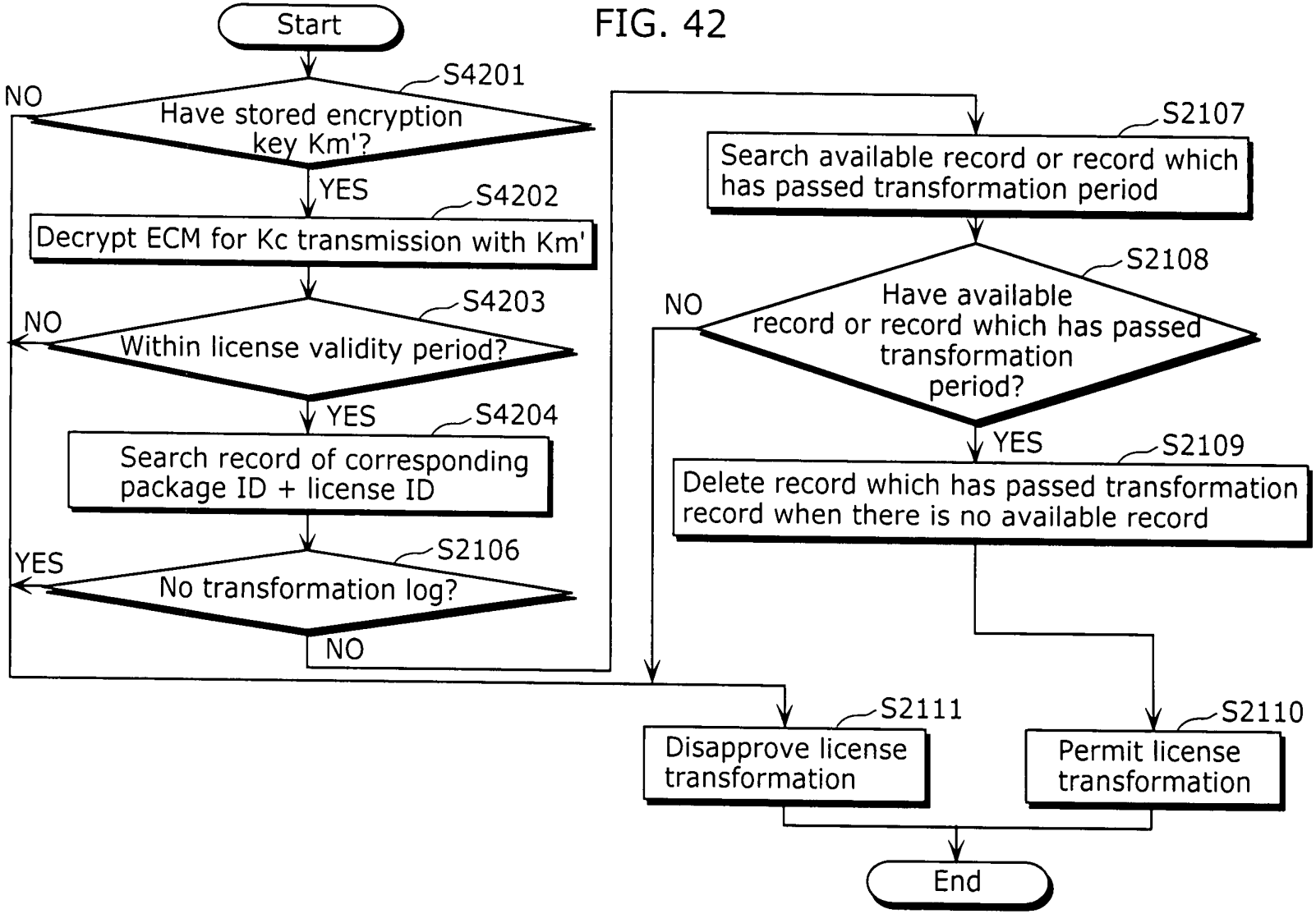

Processing in terminal apparatus 102
Start
S4101
Transmit ECM for Kc transmission to IC card
S4108
Receive response from IC card
End
Processing in IC card 103
S4102
License import permission judgment processing
S4103
Import OK?
NO
YES
S4104
Generate license from ECM for Kc transmission
S4105
Record license transformation log
S4106
Store license
S4107
Transmit response to terminal apparatus

FIG. 42


Start
S4201
Have stored encryption key Km'?
NO
YES
S4202
Decrypt ECM for Kc transmission with Km'
S4203
Within license validity period?
NO
YES
S4204
Search record of corresponding package ID + license ID
S2106
No transformation log?
YES
NO
S2107
Search available record or record which has passed transformation period
S2108
Have available record or record which has passed transformation period?
NO
YES
S2109
Delete record which has passed transformation record when there is no available record
S2111
Disapprove license transformation
S2110
Permit license transformation
End